SIEMENS

SIMATIC NET

SCALANCE W786-xPRO

Betriebsanleitung

Einleitung 1

Beschreibung 2

Montage 3

Anschließen 4

Konfigurieren/Projektieren 5

Instandhalten und Warten 6

Technische Daten 7

Anhang A

Ausgabe 08/2007
C79000-G8900-C221-02

Sicherheitshinweise

Dieses Handbuch enthält Hinweise, die Sie zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachten müssen. Die Hinweise zu Ihrer persönlichen Sicherheit sind durch ein Warndreieck hervorgehoben, Hinweise zu alleinigen Sachschäden stehen ohne Warndreieck. Je nach Gefährdungsstufe werden die Warnhinweise in abnehmender Reihenfolge wie folgt dargestellt.

⚠GEFAHR
bedeutet, dass Tod oder schwere Körperverletzung eintreten **wird**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

⚠WARNUNG
bedeutet, dass Tod oder schwere Körperverletzung eintreten **kann**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

⚠VORSICHT
mit Warndreieck bedeutet, dass eine leichte Körperverletzung eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

VORSICHT
ohne Warndreieck bedeutet, dass Sachschaden eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

ACHTUNG
bedeutet, dass ein unerwünschtes Ergebnis oder Zustand eintreten kann, wenn der entsprechende Hinweis nicht beachtet wird.

Beim Auftreten mehrerer Gefährdungsstufen wird immer der Warnhinweis zur jeweils höchsten Stufe verwendet. Wenn in einem Warnhinweis mit dem Warndreieck vor Personenschäden gewarnt wird, dann kann im selben Warnhinweis zusätzlich eine Warnung vor Sachschäden angefügt sein.

Qualifiziertes Personal

Das zugehörige Gerät/System darf nur in Verbindung mit dieser Dokumentation eingerichtet und betrieben werden. Inbetriebsetzung und Betrieb eines Gerätes/Systems dürfen nur von **qualifiziertem Personal** vorgenommen werden. Qualifiziertes Personal im Sinne der sicherheitstechnischen Hinweise dieser Dokumentation sind Personen, die die Berechtigung haben, Geräte, Systeme und Stromkreise gemäß den Standards der Sicherheitstechnik in Betrieb zu nehmen, zu erden und zu kennzeichnen.

Bestimmungsgemäßer Gebrauch

Beachten Sie Folgendes:

⚠WARNUNG
Das Gerät darf nur für die im Katalog und in der technischen Beschreibung vorgesehenen Einsatzfälle und nur in Verbindung mit von Siemens empfohlenen bzw. zugelassenen Fremdgeräten und -komponenten verwendet werden. Der einwandfreie und sichere Betrieb des Produktes setzt sachgemäßen Transport, sachgemäße Lagerung, Aufstellung und Montage sowie sorgfältige Bedienung und Instandhaltung voraus.

Marken

Alle mit dem Schutzrechtsvermerk ® gekennzeichneten Bezeichnungen sind eingetragene Marken der Siemens AG. Die übrigen Bezeichnungen in dieser Schrift können Marken sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann.

Haftungsausschluss

Wir haben den Inhalt der Druckschrift auf Übereinstimmung mit der beschriebenen Hard- und Software geprüft. Dennoch können Abweichungen nicht ausgeschlossen werden, so dass wir für die vollständige Übereinstimmung keine Gewähr übernehmen. Die Angaben in dieser Druckschrift werden regelmäßig überprüft, notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

Siemens AG
Automation and Drives
Postfach 48 48
90327 NÜRNBERG
DEUTSCHLAND

Dokumentbestellnummer: C79000-G8900-C221-02
Ⓟ 08/2007

Copyright © Siemens AG 2007.
Änderungen vorbehalten

Inhaltsverzeichnis

1 Einleitung 9

1.1 Informationen zur Betriebsanleitung SCALANCE W786-xPRO 9

1.2 Typenbezeichnungen 11

2 Beschreibung 13

2.1 Netzstrukturen 13

2.2 Lieferumfang 19

2.3 Produkteigenschaften 20

2.4 Leuchtdiodenanzeige 23

2.5 C-PLUG 26

2.6 Reset-Taster 27

2.7 Biologische Verträglichkeit 28

3 Montage 29

3.1 Demontage / Montage des Gehäusedeckels 29

3.2 Verlegung der Leitungen 32

3.3 Montage ohne Adapter (Nur Wandmontage) 35

3.4 Montage mit Halteblech 38

3.4.1 Wandmontage des Halteblechs 38

3.4.2 Aufschrauben des Abdeckblechs für die Kabelzuführung auf das Halteblech 40

3.4.3 Montage des Halteblechs auf einer S7-300-Profilschiene 42

3.4.4 Montage des Halteblechs auf einer Hutschiene 43

3.4.5 Mastmontage des Halteblechs 44

3.4.6 Montage/Demontage des SCALANCE W786 auf ein Halteblech 45

4 Anschließen 47

4.1 Blitzschutz, Versorgungsspannung und Erdung 47

4.2 Geeignete Leitungen und Antennen für den SCALANCE W786 50

4.3 Anschließen der Leitungen 52

4.4 Anschlüsse für die Stromversorgung des SCALANCE W786 56

4.5 Anschließen eines Stromversorgungsadapters 58

4.6 Anschluss für Industrial Ethernet 61

4.7 Anschlüsse für externe Antennen 62

4.8 Einsetzen / Entnehmen des C-PLUG 63

5 Konfigurieren/Projektieren 65

5.1 Technische Grundlagen 65

5.1.1 Spanning Tree 65

5.1.2 iQoS ... 66
5.1.3 Forced Roaming on IP Down ... 66
5.1.4 Link Check ... 67
5.1.5 Redundanz ... 67
5.1.6 IP-Alive ... 67
5.1.7 MAC-basierte Kommunikation ... 68
5.1.8 IP-basierte Kommunikation ... 69

5.2 Vergabe einer IP-Adresse ... 70
5.2.1 Aufbau einer IP-Adresse ... 70
5.2.2 Erstmalige Vergabe einer IP-Adresse ... 71
5.2.3 Adressvergabe über DHCP ... 72
5.2.4 Adressvergabe mit dem Primary Setup Tool ... 73

5.3 Die Wizards des Web Based Management ... 74
5.3.1 Einleitung ... 74
5.3.2 Starten des Web Based Managements und Anmeldung ... 75
5.3.3 Auswahl der Wizards ... 76

5.4 Basic Wizard ... 78
5.4.1 IP-Einstellungen ... 78
5.4.2 System Name ... 79
5.4.3 Country Code ... 80
5.4.4 Wireless-Einstellungen im Access Point-Modus ... 81
5.4.5 Wireless-Einstellungen im Client-Modus ... 82
5.4.6 Adopt MAC Address Einstellungen (Nur für Clients oder Access Points im Client-Modus) ... 83
5.4.7 Kanal-Einstellungen (Nur im Access Point-Modus) ... 86
5.4.8 Beenden des Basic Wizard ... 88

5.5 Security Wizard ... 89
5.5.1 Einleitung ... 89
5.5.2 Security-Einstellungen ... 89
5.5.3 Security-Einstellungen für die Management-Schnittstellen ... 90
5.5.4 Security-Einstellungen für das SNMP-Protokoll ... 92
5.5.5 Security-Einstellungen für WLAN (Seite 1, Nur im Access Point-Modus) ... 93
5.5.6 Security-Einstellungen für WLAN (Seite 2) ... 97
5.5.7 Einstellungen für die Sicherheitsstufe Low ... 100
5.5.8 Einstellungen für die Sicherheitsstufe Medium ... 101
5.5.9 Einstellungen für die Sicherheitsstufe High im Access Point-Modus ... 102
5.5.10 Einstellungen für die Sicherheitsstufe High für die Betriebsart "Client" ... 103
5.5.11 Übersicht der gewählten Sicherheitseinstellungen für einen Access Point ... 104
5.5.12 Beenden des Security Wizards ... 105

5.6 Konfiguration über das Web Based Management ... 106
5.6.1 Allgemeine Informationen zum Web Based Management ... 106
5.6.2 Leuchtdiodensimulation des Web Based Management ... 107
5.6.3 Das Menü System ... 108
5.6.3.1 Menüpunkt System Information ... 108
5.6.3.2 Menüpunkt IP Einstellungen ... 109
5.6.3.3 Menüpunkt Services ... 109
5.6.3.4 Menüpunkt Restart ... 110
5.6.3.5 Menüpunkt Event Config ... 111
5.6.3.6 Menüpunkt E-Mail Config ... 113
5.6.3.7 Menüpunkt SNMP Config ... 113
5.6.3.8 Menüpunkt Syslog ... 115
5.6.3.9 Menüpunkt SNTP Config ... 117
5.6.3.10 Menüpunkt Fault State ... 117
5.6.3.11 Menüpunkt Load & Save ... 118

5.6.3.12 Menüpunkt C-PLUG....121
5.6.4 Das Menü Interfaces....125
5.6.4.1 Menüpunkt Interfaces....125
5.6.4.2 Menüpunkt Ethernet....125
5.6.4.3 Menüpunkt WLAN....126
5.6.4.4 Menüpunkt Advanced....129
5.6.4.5 Menüpunkt SSID List....133
5.6.4.6 Menüpunkt Advanced G....134
5.6.4.7 Menüpunkt Data Rates....135
5.6.4.8 Menüpunkt VAP....136
5.6.5 Das Menü Security....137
5.6.5.1 Menüpunkt Security....137
5.6.5.2 Menüpunkt Basic Wireless....137
5.6.5.3 Menüpunkt Keys....142
5.6.5.4 Menüpunkt ACL....143
5.6.5.5 Menüpunkt RADIUS Server....145
5.6.5.6 Menüpunkt Access....146
5.6.6 Das Menü Bridge....147
5.6.6.1 Menüpunkt Bridge....147
5.6.6.2 Menüpunkt WDS....148
5.6.6.3 Menüpunkt VLAN....151
5.6.6.4 Menüpunkt Learning Table....158
5.6.6.5 Menüpunkt ARP Table....158
5.6.6.6 Menüpunkt Spanning Tree....158
5.6.6.7 Menüpunkt Storm Threshold....166
5.6.6.8 Menüpunkt NAT....166
5.6.6.9 Menüpunkt IP Mapping Table....170
5.6.7 Das Menü Filters....172
5.6.7.1 Menüpunkt Filters....172
5.6.7.2 Menüpunkt MAC Filters....172
5.6.7.3 Menüpunkt MAC Dir Filter....172
5.6.7.4 Menüpunkt Protocol Filter....173
5.6.8 Das Menü I-Features....173
5.6.8.1 Menüpunkt I-Features....173
5.6.8.2 Menüpunkt iQoS (Nur im Access Point-Modus)....174
5.6.8.3 Menüpunkt Forced Roaming on IP Down (Nur im Access Point-Modus)....175
5.6.8.4 Menüpunkt Link Check (Nur im Access Point-Modus)....175
5.6.8.5 Menüpunkt Redundancy (Nur im Access Point-Modus)....176
5.6.8.6 Menüpunkt IP Alive (Nur im Access Point-Modus)....177
5.6.9 Das Menü Information....178
5.6.9.1 Menüpunkt Information....178
5.6.9.2 Menüpunkt Log Table....178
5.6.9.3 Menüpunkt Auth Log....179
5.6.9.4 Menüpunkt Versions....179
5.6.9.5 Menüpunkt Client List....181
5.6.9.6 Menüpunkt Ethernet....183
5.6.9.7 Menüpunkt WLAN....183
5.6.9.8 Menüpunkt iQoS....188
5.6.9.9 Menüpunkt Spanning Tree....189
5.6.9.10 Menüpunkt IP, TCP/IP, IPCM, SNMP....191
5.6.9.11 Menüpunkt Signal Recorder....191

5.7 Konfiguration mit dem Command Line Interface....195
5.7.1 Allgemeine Informationen über das Command Line Interface....195
5.7.2 Das Menü CLI\SYSTEM....198
5.7.2.1 Menüpunkt CLI\SYSTEM....198

5.7.2.2 Menüpunkt CLI\SYSTEM\IP ... 199
5.7.2.3 Menüpunkt CLI\SYSTEM\SERVICES ... 200
5.7.2.4 Menüpunkt CLI\SYSTEM\RESTARTS ... 201
5.7.2.5 Menüpunkt CLI\SYSTEM\EVENT ... 202
5.7.2.6 Menüpunkt CLI\SYSTEM\EMAIL ... 205
5.7.2.7 Menüpunkt CLI\SYSTEM\SNMP ... 206
5.7.2.8 Menüpunkt CLI\SYSTEM\SNMP\GROUP ... 207
5.7.2.9 Menüpunkt CLI\SYSTEM\SNMP\USER ... 209
5.7.2.10 Menüpunkt CLI\SYSTEM\SNMP\TRAP ... 210
5.7.2.11 Menüpunkt CLI\SYSTEM\SYSLOG ... 211
5.7.2.12 Menüpunkt CLI\SYSTEM\SNTP ... 212
5.7.2.13 Menüpunkt CLI\SYSTEM\FAULT ... 213
5.7.2.14 Menüpunkt CLI\SYSTEM\LOADSAVE ... 214
5.7.2.15 Menüpunkt CLI\SYSTEM\CPLUG ... 216
5.7.3 Das Menü CLI\INTERFACES ... 217
5.7.3.1 Menüpunkt CLI\INTERFACES\ETHERNET ... 217
5.7.3.2 Menüpunkt CLI\INTERFACES\WLAN1 (bzw. \WLAN2 oder \WLAN3) ... 218
5.7.3.3 Menüpunkt CLI\INTERFACES\WLAN1\ADVANCED (bzw. \WLAN2\ADVANCED oder \WLAN3\ADVANCED) ... 220
5.7.3.4 Menüpunkt CLI\INTERFACES\WLAN1\SSID (bzw. \WLAN2\SSID oder \WLAN3\SSID) ... 223
5.7.3.5 Menüpunkt CLI\INTERFACES\WLAN1\802.11G (bzw. \WLAN2\802.11G oder \WLAN3\802.11G) ... 224
5.7.3.6 Menüpunkt CLI\INTERFACES\WLAN1\DATARATES (bzw. \WLAN2\DATARATES oder \WLAN3\DATARATES) ... 225
5.7.3.7 Menüpunkt CLI\INTERFACES\WLAN1\VAP1..7 (bzw. \WLAN2\VAP1..7 oder \WLAN3\VAP1..7) ... 226
5.7.4 Das Menü CLI\SECURITY ... 227
5.7.4.1 Menüpunkt CLI\SECURITY ... 227
5.7.4.2 Menüpunkt CLI\SECURITY\BASIC\WLAN1 (bzw. \WLAN2 oder \WLAN3) ... 228
5.7.4.3 Menüpunkt CLI\SECURITY\BASIC\WLAN1\VAP1..7 (bzw. \WLAN2\VAP1..7 oder \WLAN3\VAP1..7) ... 230
5.7.4.4 Menüpunkt CLI\SECURITY\KEYS\WLAN1 (bzw. \WLAN2 oder \WLAN3) ... 231
5.7.4.5 Menüpunkt CLI\SECURITY\ACL\WLAN1 (bzw. \WLAN2 oder \WLAN3) ... 232
5.7.4.6 Menüpunkt CLI\SECURITY\RADIUS ... 233
5.7.4.7 Menüpunkt CLI\SECURITY\ACCESS ... 234
5.7.5 Das Menü CLI\BRIDGE ... 235
5.7.5.1 Menüpunkt CLI\BRIDGE ... 235
5.7.5.2 Menüpunkt CLI\BRIDGE\WDS\WLAN1 (bzw. \WLAN2 oder \WLAN3) ... 236
5.7.5.3 Menüpunkt CLI\BRIDGE\VLAN\VLAN_ID ... 237
5.7.5.4 Menüpunkt CLI\BRIDGE\VLAN\PORTS ... 238
5.7.5.5 Menüpunkt CLI\BRIDGE\SPANNING ... 239
5.7.5.6 Menüpunkt CLI\BRIDGE\SPANNING\PORTS ... 240
5.7.5.7 Menüpunkt CLI\BRIDGE\STORMTHR ... 241
5.7.5.8 Menüpunkt CLI\BRIDGE\NAT ... 241
5.7.5.9 Menüpunkt CLI\BRIDGE\NAT\STATIC ... 243
5.7.6 Das Menü CLI\FILTERS ... 244
5.7.6.1 Menüpunkt CLI\FILTERS\MAC1FLT ... 244
5.7.6.2 Menüpunkt CLI\FILTERS\MAC2FLT ... 245
5.7.6.3 Menüpunkt CLI\FILTERS\PROTO ... 246
5.7.7 Das Menü CLI\IFEATURES ... 247
5.7.7.1 Menüpunkt CLI\IFEATURES\IQOS\WLAN1 (bzw. \WLAN2 oder \WLAN3) ... 247
5.7.7.2 Menüpunkt CLI\IFEATURES\FORCED_ROAM\WLAN1 (bzw. \WLAN2 oder \WLAN3) ... 249
5.7.7.3 Menüpunkt CLI\IFEATURES\LINKCHECK ... 250
5.7.7.4 Menüpunkt CLI\IFEATURES\REDUNDANCY ... 251
5.7.7.5 Menüpunkt CLI\IFEATURES\IP_ALIVE ... 252

5.7.8 Das Menü CLI\INFORM 253
5.7.8.1 Menüpunkt CLI\INFORM 253
5.7.8.2 Menüpunkt CLI\INFORM\LOG 254
5.7.8.3 Menüpunkt CLI\INFORM\AUTHLOG 255
5.7.8.4 Menüpunkt CLI\INFORM\WLAN1 (bzw. \WLAN2 oder \WLAN3) 256
5.7.8.5 Menüpunkt CLI\INFORM\SIGNAL 257

5.8 Konfiguration mit dem PRESET-PLUG 258
5.8.1 Funktionsprinzip des PRESET-PLUG 258
5.8.2 Erstellen einer Konfiguration mit einem neuen PRESET-PLUG 258
5.8.3 Ändern eines PRESET-PLUG, der bereits Konfigurationsdaten enthält 260
5.8.4 Inbetriebnahme eines Geräts mit einem PRESET-PLUG 260

6 Instandhalten und Warten 263

6.1 Laden einer neuen Firmware über FTP 263

6.2 Wiederherstellen der Default-Parameter 264

7 Technische Daten 265

7.1 Technische Daten SCALANCE W786 265

A Anhang 269

A.1 Private MIB-Variablen des SCALANCE W78x / W74x 269

A.2 Auslegung und Berechnung von Funksystemen (Beispiel RCoax) 273

Glossar 281

Index 289

1 Einleitung

1.1 Informationen zur Betriebsanleitung SCALANCE W786-xPRO

Gültigkeitsbereich dieser Betriebsanleitung

Diese Betriebsanleitung behandelt die folgenden Produkte:

- SCALANCE W786-1PRO
- SCALANCE W786-2PRO
- SCALANCE W786-3PRO

Die Betriebsanleitung gilt für folgende Software-Version:

- SCALANCE W786-xPRO Firmware ab Version 3.3

Hinweis

Diese Betriebsanleitung gilt nicht für den SCALANCE W786-2HPW.

Zweck dieser Betriebsanleitung

Diese Betriebsanleitung soll Sie in die Lage versetzen, den SCALANCE W786-xPRO fachgerecht zu montieren, in Betrieb zu nehmen und zu bedienen. Es vermittelt die notwendigen Kenntnisse über die Konfiguration des SCALANCE W786-xPRO sowie die Einbindung des SCALANCE W786-xPRO in ein WLAN-Netz.

Einordnung in die Dokumentationslandschaft

Zum Thema Industrial Wireless LAN gibt es von SIMATIC NET außer der Betriebsanleitung, die Sie gerade lesen, noch folgende Dokumentation:

- Betriebsanleitung (kompakt) SCALANCE W786-xPRO

  Dieses Dokument liegt in Papierform dem Gerät bei und enthält eine komprimierte Zusammenstellung der wichtigsten Informationen für die Nutzung der folgenden Produkte:

  – SCALANCE W786-1PRO
  – SCALANCE W786-2PRO
  – SCALANCE W786-3PRO

- Betriebsanleitung SCALANCE W788-xPRO/RR / SCALANCE W74x-1PRO/RR
  Die ausführliche Benutzerdokumentation für die folgenden Produkte:

  - SCALANCE W788-1PRO
  - SCALANCE W788-2PRO
  - SCALANCE W788-1RR
  - SCALANCE W788-2RR
  - SCALANCE W744-1PRO
  - SCALANCE W746-1PRO
  - SCALANCE W747-1RR

  Das Dokument enthält alle Informationen für den Aufbau, die Inbetriebnahme und den Betrieb dieser Geräte.

- Betriebsanleitung SCALANCE W784-1xx / SCALANCE W74x-1
  Die ausführliche Benutzerdokumentation für die folgenden Produkte:
  - SCALANCE W784-1
  - SCALANCE W784-1RR
  - SCALANCE W744-1
  - SCALANCE W746-1
  - SCALANCE W747-1

  Das Dokument enthält alle Informationen für den Aufbau, die Inbetriebnahme und den Betrieb dieser Geräte.

- Systemhandbuch Grundlagen Wireless LAN

  Es enthält neben der Beschreibung der physikalischen Grundlagen und einer Darstellung der wichtigsten IEEE-Standards auch Informationen über die Datensicherheit und eine Beschreibung von Industrieanwendungen von Wireless LAN.
  Sie sollten dieses Handbuch lesen, wenn Sie WLAN-Netze mit einer komplexeren Struktur aufbauen wollen (nicht nur Verbindung zwischen zwei Geräten).

- Systemhandbuch RCoax

  Dieses Systemhandbuch enthält sowohl eine Erklärung der technischen Grundlagen von Leckwellenleitern als auch eine Beschreibung der SIMATIC NET RCoax-Komponenten und deren Arbeitsweise. Die Montage / Inbetriebnahme sowie der Anschluss von RCoax-Komponenten wird erläutert.

- Handbuch Netzübergang IWLAN/PB LINK PNIO für Industrial Ethernet

  Die Benutzerdokumentation für den IWLAN/PB LINK PNIO. Dieses Gerät ist ein Netzübergang zwischen IWLAN und PROFIBUS.

1.2 Typenbezeichnungen

Verwendete Abkürzungen

Die Informationen in den Handbüchern der SCALANCE W-700-Produktfamilie gelten häufig nicht nur für eine Produktvariante. In diesen Fällen werden abkürzende Bezeichnungen verwendet, um nicht alle Typenbezeichnungen aufzählen zu müssen. Die folgende Tabelle zeigt die Zuordnung von Abkürzungen und Produktvarianten.

Produktgruppe	Die Bezeichnung . . . steht für . . .	Produktname
Ethernet Client Module (IP30, Schaltschrankeinbau)	W74x-1	W744-1 W746-1 W747-1
Ethernet Client Module (IP65, Aufstellung außerhalb eines Schaltschranks)	W74x-1PRO/RR	W744-1PRO W746-1PRO W747-1RR
Alle Ethernet Client Module SCALANCE W	W74x	W744-1 W746-1 W747-1 W744-1PRO W746-1PRO W747-1RR
Access Points (IP30, Schaltschrankeinbau)	W784-1xx	W784-1 W784-1RR
Access Points (IP65, Aufstellung außerhalb eines Schaltschranks, hohe klimatische Anforderungen)	W786-xPRO	W786-1PRO W786-2PRO W786-3PRO
Access Points (IP65, Aufstellung außerhalb eines Schaltschranks)	W788-xPRO/RR	W788-1PRO W788-2PRO W788-1RR W788-2RR
Access Points mit dem Funktionsumfang "RR"	W-78x-xRR	W784-1RR W788-1RR W788-2RR
Alle Access Points SCALANCE W	W78x	W788-1PRO W788-2PRO W788-1RR W788-2RR W786-1PRO W786-2PRO W786-3PRO W784-1 W784-1RR

Produktgruppe	Die Bezeichnung . . . steht für . . .	Produktname
Alle SCALANCE W	W-700	W788-1PRO W788-2PRO W788-1RR W788-2RR W744-1PRO W746-1PRO W747-1RR W786-1PRO W786-2PRO W786-3PRO W784-1 W784-1RR W744-1 W746-1 W747-1

Beschreibung

2

2.1 Netzstrukturen

Standalone-Konfiguration mit dem SCALANCE W78x

Diese Konfiguration erfordert keinen Server und der SCALANCE W78x verfügt nicht über eine Verbindung zu einem drahtgebundenen Ethernet. Der SCALANCE W78x leitet innerhalb seiner Reichweite Daten von einem WLAN-Teilnehmer zu einem anderen.

Das Funknetz hat einen eindeutigen Namen. Alle Geräte, die innerhalb dieses Netzes Daten austauschen wollen, müssen mit diesem Namen konfiguriert sein.

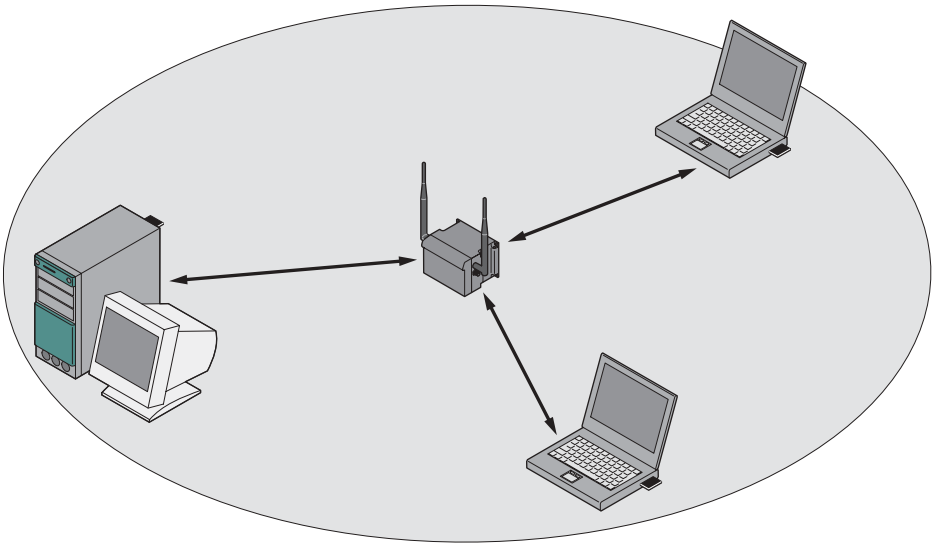


Bild 2-1 Standalone-Konfiguration eines SCALANCE W78x. Die graue Fläche symbolisiert dabei die Funkreichweite des SCALANCE W78x.

Ad-Hoc-Netzwerke

Im Ad-Hoc-Modus kommunizieren die Teilnehmer direkt miteinander (Verbindung 4) ohne Einbeziehung eines SCALANCE W78x. Die Teilnehmer greifen auf gemeinsame Ressourcen (Dateien oder auch Geräte, z. B. Drucker) des Servers zu (Verbindungen 1 bis 3 in der Abbildung). Voraussetzung dafür ist natürlich, dass sich die Teilnehmer in der Funkreichweite des Servers oder in der gegenseitigen Funkreichweite befinden.

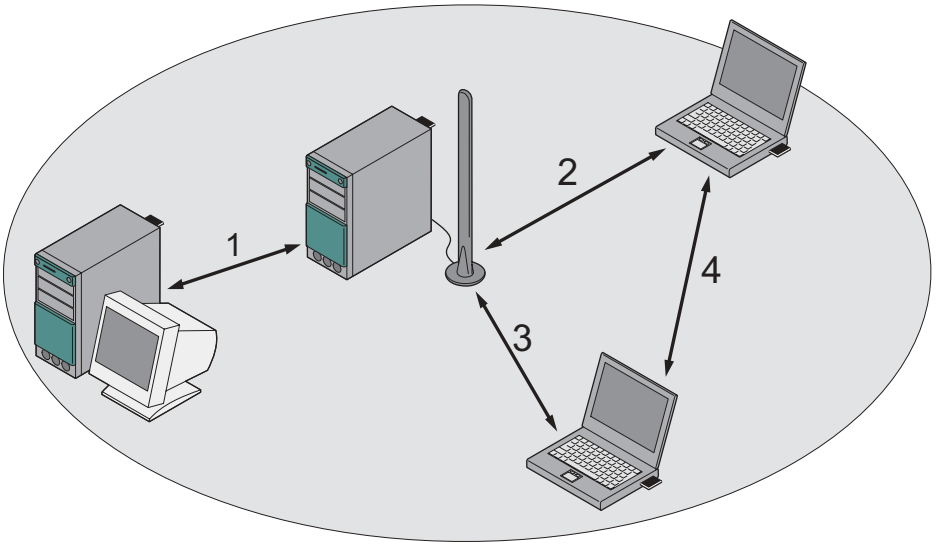


Bild 2-2 Ad-Hoc-Netzwerk ohne SCALANCE W78x

Funkzugang zu einem drahtgebundenen Ethernet-Netzwerk

Wenn ein (oder mehrere) SCALANCE W78x Verbindung zu einem drahtgebundenen Ethernet haben, bieten sich folgende Einsatzmöglichkeiten an:

- Ein einzelner SCALANCE W78x als Netzübergang:

  Ein drahtloses Netz kann mit einem drahtgebundenen Netz über einen SCALANCE W78x verbunden werden.

- Ausdehnung der Funkabdeckung für das drahtlose Netz mit mehreren SCALANCE W78x:

  Die SCALANCE W78x sind alle mit der gleichen eindeutigen SSID (Netznamen) konfiguriert. Alle Teilnehmer, die über dieses Netz kommunizieren wollen, müssen ebenfalls mit dieser SSID konfiguriert sein.

  Wird eine mobile Station aus dem Bereich eines SCALANCE W78x in den Bereich eines anderen SCALANCE W78x verschoben, bleibt die Funkverbindung bestehen (Roaming).

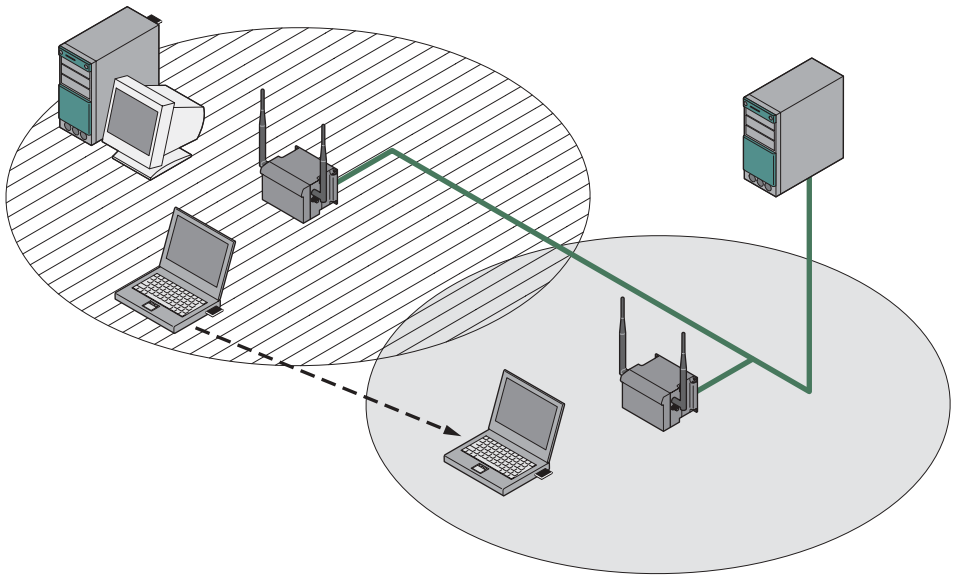


Bild 2-3 Funkverbindung einer mobilen Station über zwei Funkzellen (Roaming)

Mehrkanal-Konfiguration

Nutzen benachbarte SCALANCE W78x den gleichen Frequenzkanal, kommt es wegen der auftretenden Kollisionen zu längeren Antwortzeiten. Würde die in der Abbildung dargestellte Konfiguration als Einkanal-System realisiert, könnten Computer A und B nicht gleichzeitig mit den entsprechenden SCALANCE W78x in ihrer Funkzelle kommunizieren.

Wenn benachbarte SCALANCE W78x für unterschiedliche Frequenzen eingerichtet werden, führt das zu einer erheblichen Performance-Verbesserung. Dadurch wird benachbarten Funkzellen jeweils ein eigenes Medium zur Verfügung gestellt, und die Verzögerungen durch zeitversetztes Senden entfallen.

Der Kanalabstand sollte möglichst groß sein, ein sinnvoller Wert ist 25 MHz (fünf Kanäle). Auch bei der Mehrkanal-Konfiguration können alle SCALANCE W78x mit dem gleichen Netznamen konfiguriert werden.

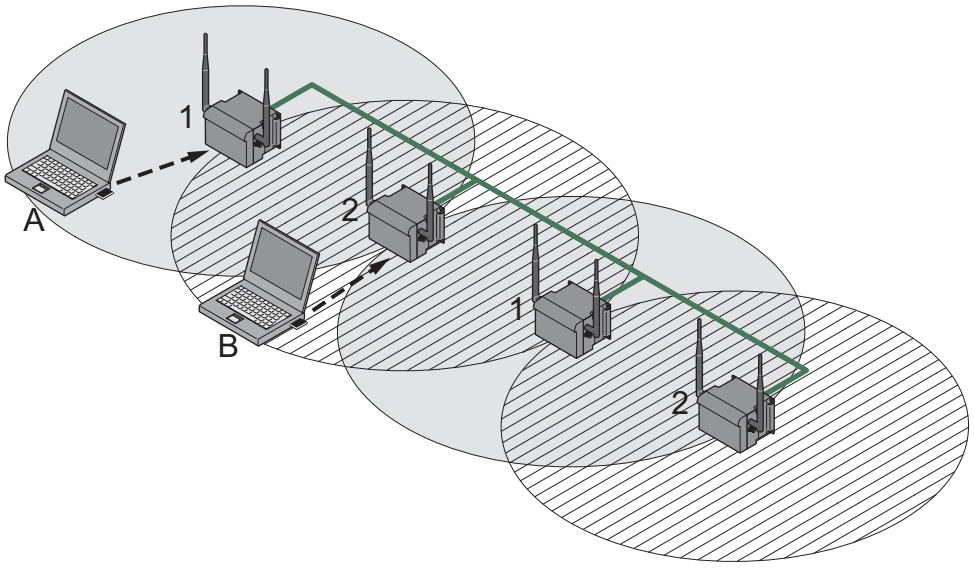


Bild 2-4 Mehrkanalkonfiguration auf den Kanälen 1 und 7 mit vier SCALANCE W78x

Wireless Distribution System (WDS)

WDS ermöglicht direkte Verbindungen zwischen SCALANCE W78x-Geräten oder zwischen SCALANCE W78x und anderen WDS-fähigen Geräten. Sie dienen zum Aufbau eines Wireless Backbone oder zur Anbindung eines einzelnen SCALANCE W78x an ein Netzwerk, der auf Grund seiner Lage nicht direkt an die Kabelinfrastruktur angeschlossen werden kann.

Bei der Konfiguration bieten sich zwei Alternativen. Der WDS-Partner kann sowohl über seinen Namen als auch über seine MAC-Adresse konfiguriert werden.

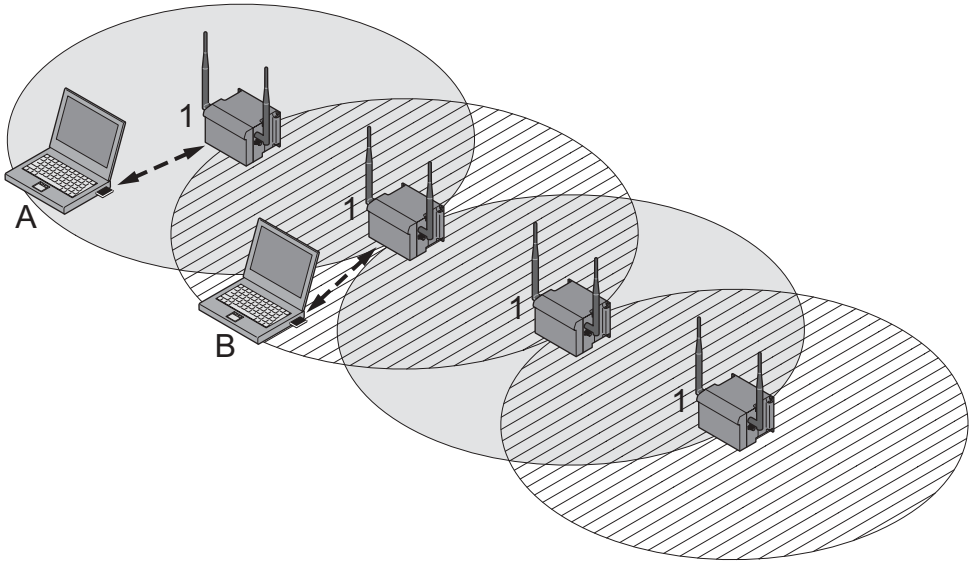


Bild 2-5 Realisierung von WDS mit vier SCALANCE W78x

Redundant Wireless LAN (RWLAN)

RWLAN ermöglicht eine redundante, drahtlose Verbindung zwischen zwei SCALANCE W78x-Geräten mit mindestens zwei WLAN-Schnittstellen. Dies dient zum Aufbau eines redundanten Wireless Backbone, welches auf Grund seiner Lage nicht als verkabeltes Netz aufgebaut werden kann, jedoch trotzdem erhöhte Anforderungen bzgl. der Verfügbarkeit besitzt.

Bei der Konfiguration bieten sich zwei Alternativen. Der RWLAN-Partner kann sowohl über seinen Namen als auch über seine MAC-Adresse konfiguriert werden.

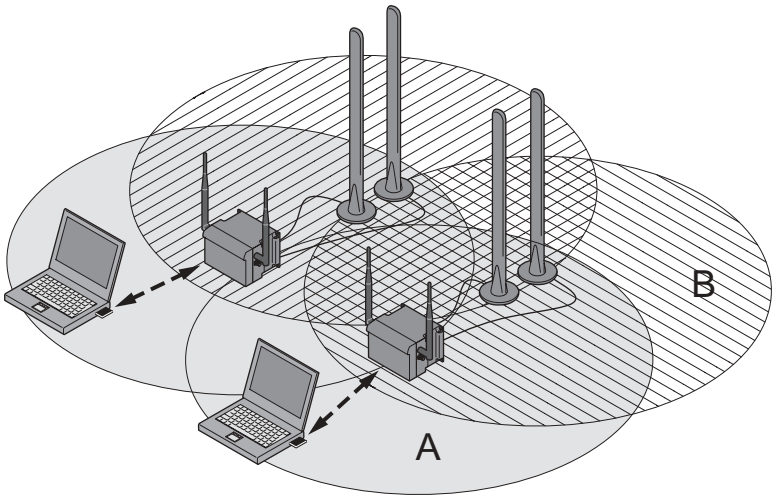


Bild 2-6 Realisierung von RWLAN mit zwei SCALANCE W78x-Geräten mit mindestens zwei WLAN-Schnittstellen. Der Datentransfer kann alternativ über eine der beiden Funkkarten erfolgen.

2.2 Lieferumfang

Folgende Teile gehören zum Lieferumfang des SCALANCE W786:

- SCALANCE W786
- 5 Verschlusskappen für die Deckelverschraubung
- Ausführungsabhängig bis zu 8 Stopfen für die Gehäusedichtung
- Ausführungsabhängig bis zu 8 Zugentlastungsklammern
- 1 Stecker für die DC 48V-Spannungsversorgung
- 2 Dichtungsklebefolien für ovale Lichtwellenleiter
  (entfällt bei Geräten mit einer RJ45-Schnittstelle)
- 1 SIMATIC NET Industrial Wireless LAN CD mit der vorliegenden Betriebsanleitung für den SCALANCE W78x
- 1 Betriebsanleitung kompakt SCALANCE W786

Überprüfen Sie die Vollständigkeit der Lieferung. Setzen Sie sich bei unvollständiger Lieferung mit Ihrem Lieferanten oder der örtlichen Siemens-Geschäftsstelle in Verbindung.

2.3 Produkteigenschaften

Einsatzmöglichkeiten für den SCALANCE W786

Der SCALANCE W786 ist mit einer Ethernet-Schnittstelle und bis zu drei Wireless-LAN-Schnittstellen ausgestattet. Dadurch ist dieses Gerät für folgende Einsatzfälle geeignet:

- Der SCALANCE W786 leitet innerhalb seiner Reichweite Daten von einem Teilnehmer zu einem anderen, ohne dass eine Verbindung zu einem drahtgebundenen Ethernet bestehen muss.
- Der SCALANCE W786 kann als Netzübergang von einem drahtgebundenen zu einem drahtlosen Netz verwendet werden.
- Der SCALANCE W786 kann als drahtlose Brücke zwischen zwei Netzen eingesetzt werden.
- Der SCALANCE W786 kann als Brücke zwischen zwei Funkzellen mit verschiedenen Frequenzen dienen.

Darüber hinaus können Sie mit einem SCALANCE W786 mit mehr als einer WLAN-Schnittstelle auch eine redundante Funkverbindung zu einem SCALANCE W78x mit mindestens zwei WLAN-Schnittstellen realisieren.

Eigenschaften des SCALANCE W786

- Die Ethernet-Schnittstelle unterstützt 10 Mbit/s und 100 Mbit/s, jeweils Voll-Duplex und Halb-Duplex sowie Auto-Crossing und Auto-Polarity.
- Betrieb der drahtlosen Schnittstelle in den Frequenzbändern 2,4 GHz und 5 GHz.
- Die drahtlose Schnittstelle ist kompatibel zu den Standards IEEE 802.11a, IEEE 802.11h, IEEE 802.11b und IEEE 802.11g. Im 802.11a-, 802.11h- und 802.11g-Modus beträgt die Brutto-Übertragungsgeschwindigkeit bis zu 54 Mbit/s. Im Turbo-Modus beträgt die Übertragungsgeschwindigkeit bis zu 108 Mbit/s (nicht in allen Ländern und Betriebsarten erlaubt).
- Als Erweiterung des 802.11a-Modus steht außerdem der Betrieb gemäß dem Standard IEEE 802.11h zur Verfügung. Im 802.11h-Modus werden die beiden Verfahren Transmit Power Control (TPC) sowie Dynamic Frequency Selection (DFS) im Bereich von 5,25 - 5,35 und 5,47 - 5,75 GHz verwendet. Dadurch kann in einigen Ländern das Frequenz-Subband von 5,47 - 5,725 GHz im Outdoor-Bereich auch mit höheren Sendeleistungen genutzt werden.
  TPC ist ein Verfahren zur Steuerung der Sendeleistung, die auf das aktuell notwendige Maß reduziert wird. Bei der dynamischen Frequenzbandwahl (DFS) sucht der Access Point vor Aufnahme der Kommunikation einen zufällig gewählten Kanal nach Primärnutzern (z.B. Radar) ab. Werden Signale auf dem Kanal entdeckt, dann ist dieser Kanal für 30 Minuten gesperrt und die Verfügbarkeitsprüfung wird auf einem anderen Kanal wiederholt.
- Unterstützung der Authentifizierungs-Standards WPA, WPA-PSK, WPA2, WPA2-PSK und IEEE 802.1x sowie der Verschlüsselungsverfahren WEP, AES und TKIP.
- Geeignet für die Einbeziehung eines RADIUS-Servers für die Authentifizierung.
- Gerätebezogene und anwendungsbezogene Überwachung der Funkverbindung.
- Die Interoperabilität der-Geräte mit Wi-Fi-Geräten anderer Hersteller wurde ausführlich getestet.

Hinweis

Im Client-Modus können Sie einen SCALANCE W786-xPRO mit der Funktion eines SCALANCE W746-1PRO einsetzen.

Die folgende Tabelle zeigt die Unterschiede zwischen den verschiedenen Modellvarianten des SCALANCE W786:

Typ	Anzahl der WLAN-Schnittstellen	Anzahl und Art der Ethernet-Schnittstellen	Anzahl interne Antennen	Anzahl R-SMA-Buchsen für externe Antennen	Bestell-Nr.
W786-1PRO	1	1 RJ45	1 (Diversity(2))	—	6GK5786-1BA60-2AA0 6GK5786-1BA60-2AB0 (1)
W786-1PRO	1	1 RJ45	—	2	6GK5786-1AA60-2AA0 6GK5786-1AA60-2AB0 (1)
W786-1PRO	1	1 ST Duplex Multimode Lichtwellen-leiter	1 (Diversity(2))	—	6GK5786-1BB60-2AA0 6GK5786-1BB60-2AB0 (1)
W786-1PRO	1	1 ST Duplex Multimode Lichtwellen-leiter	—	2	6GK5786-1AB60-2AA0 6GK5786-1AB60-2AB0 (1)
W786-2PRO	2	1 RJ45	2 (Diversity(2))	—	6GK5786-2BA60-2AA0 6GK5786-2BA60-2AB0 (1)
W786-2PRO	2	1 RJ45	—	4	6GK5786-2AA60-2AA0 6GK5786-2AA60-2AB0 (1)
W786-2PRO	2	1 ST Duplex Multimode Lichtwellenleiter	2 (Diversity(2))	—	6GK5786-2BB60-2AA0 6GK5786-2BB60-2AB0 (1)

Typ	Anzahl der WLAN-Schnittstellen	Anzahl und Art der Ethernet-Schnittstellen	Anzahl interne Antennen	Anzahl R-SMA-Buchsen für externe Antennen	Bestell-Nr.
W786-2PRO	2	1 ST Duplex Multimode Lichtwellen-leiter	—	4	6GK5786-2AB60-2AA0 6GK5786-2AB60-2AB0 (1)
W786-3PRO	3	1 RJ45	—	6	6GK5786-3AA60-2AA0 6GK5786-3AA60-2AB0 (1)
W786-3PRO	3	1 ST Duplex Mulitmode Lichtwellen-leiter	—	6	6GK5786-3AB60-2AA0 6GK5786-3AB60-2AB0 (1)

(1) US-Variante

(2) Pro WLAN-Schnittstelle gibt es zwei interne Antennen. Es wird immer die verwendet, die die bestmögliche Datenübertragung gewährleistet (Diversity).

Voraussetzungen für Installation und Betrieb

Es muss ein PG/PC mit Netzwerkanschluss für die Konfiguration des SCALANCE W786 vorhanden sein. Falls kein DHCP-Server zur Verfügung steht, ist für die erstmalige Zuordnung einer IP-Adresse an den SCALANCE W786 ein PC erforderlich, auf dem das Primary Setup Tool (PST) installiert ist. Für die weitere Konfiguration ist ein Computer mit Telnet oder einem Internet-Browser notwendig.

2.4 Leuchtdiodenanzeige

Informationen über Betriebszustand und Datentransfer

Auf der Vorderseite des Gehäuses informieren mehrere Leuchtdioden über den Betriebszustand des SCALANCE W786:

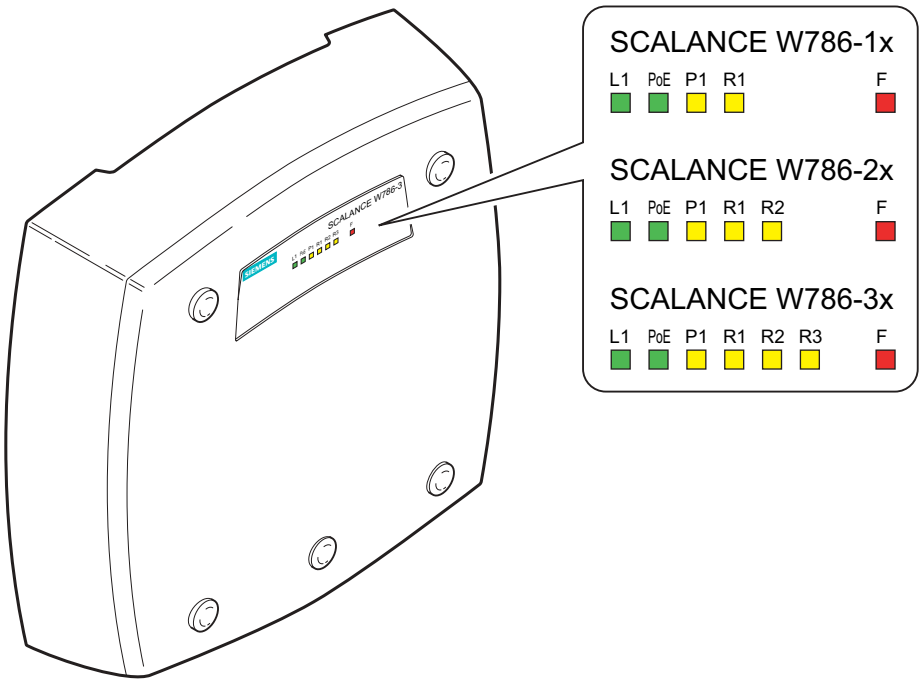


Bild 2-7 Die Leuchtdiodenanzeige des SCALANCE W786

Hinweis

Die Leuchtdiode "PoE" ist bei Geräten mit einer Schnittstelle für Lichtwellenleiter nicht vorhanden.

LED	Farbe	Bedeutung
L1	Grün	Spannungsversorgung über einen Stromversorgungsadapter oder die DC 48 V-Energiekontakte bei Geräten mit einer Schnittstelle für Lichtwellenleiter.
PoE	Grün	Spannungsversorgung über Power over Ethernet oder die DC 48 V-Energiekontakte bei Geräten mit einer RJ45-Schnittstelle.
P1	Gelb	Datentransfer über die Ethernet-Schnittstelle (Traffic).
	Grün	Es besteht eine Verbindung über die Ethernet-Schnittstelle. (Link).
	Gelb blinkend	PRESET-PLUG erkannt.
	Gelb/Grün	PRESET-Funktion erfolgreich beendet.
	Grün blinkend	"Blinken" über PST aktiviert.
R1	Gelb	Datentransfer über die erste WLAN-Schnittstelle.
	Grün	*Access Point Mode:* Die WLAN-Schnittstelle ist initialisiert und bereit. *Client Mode:* Es besteht eine Verbindung über die erste WLAN-Schnittstelle.
	Grün blinkend	*Access Point Mode:* Die Kanäle werden "gescannt". *Client Mode:* Der Client sucht die Verbindung mit einem Access Point oder Ad-Hoc Netzwerk.
	Grün schnell blinkend	*Access Point Mode:* Bei 802.11h wird eine Minute nach Primärnutzern auf dem Kanal gescannt, bevor der Kanal für den Datenverkehr genutzt werden kann. *Client Mode:* Der Client wartet auf die Adopt-MAC-Adresse durch die Einstellung <Auto Find Adopt MAC> und ist mit keinem Access Point verbunden.
	Grün 3x schnell, 1x lang blinkend	*Client Mode:* Der Client wartet auf die Adopt-MAC-Adresse durch die Einstellung <Auto Find Adopt MAC> und ist mit einem Access Point verbunden.
	Gelb blinkend	PRESET-PLUG erkannt.
	Gelb/Grün	PRESET-Funktion erfolgreich beendet.
R2	Gelb	*Access Point Mode:* Datentransfer über die zweite WLAN-Schnittstelle. *Client Mode:* Die LED ist immer aus, da die 2. Schnittstelle im Client-Modus nicht verfügbar ist.
	Grün	*Access Point Mode:* Die WLAN-Schnittstelle ist initialisiert und bereit. *Client Mode:* Die LED ist immer aus, da die 2. Schnittstelle im Client-Modus nicht verfügbar ist.
	Grün blinkend	*Access Point Mode:* Die Kanäle werden "gescannt". *Client Mode:* Die LED ist immer aus, da die 2. Schnittstelle im Client-Modus nicht verfügbar ist.

LED	Farbe	Bedeutung
	Grün schnell blinkend	*Access Point Mode:* Bei 802.11h wird eine Minute nach Primärnutzern auf dem Kanal gescannt, bevor der Kanal für den Datenverkehr genutzt werden kann. *Client Mode:* Die LED ist immer aus, da die 2. Schnittstelle im Client Mode nicht verfügbar ist.
	Gelb blinkend	PRESET-PLUG erkannt.
	Gelb/Grün	PRESET-Funktion erfolgreich beendet.
R3	Gelb	*Access Point Mode:* Datentransfer über die dritte WLAN-Schnittstelle. *Client Mode:* Die LED ist immer aus, da die 3. Schnittstelle im Client-Modus nicht verfügbar ist.
	Grün	*Access Point Mode:* Die WLAN-Schnittstelle ist initialisiert und bereit. *Client Mode:* Die LED ist immer aus, da die 3. Schnittstelle im Client-Modus nicht verfügbar ist.
	Grün blinkend	*Access Point Mode:* Die Kanäle werden "gescannt". *Client Mode:* Die LED ist immer aus, da die 3. Schnittstelle im Client-Modus nicht verfügbar ist.
	Grün schnell blinkend	*Access Point Mode:* Bei 802.11h wird eine Minute nach Primärnutzern auf dem Kanal gescannt, bevor der Kanal für den Datenverkehr genutzt werden kann. *Client Mode:* Die LED ist immer aus, da die 3. Schnittstelle im Client Mode nicht verfügbar ist.
	Gelb blinkend	PRESET-PLUG erkannt.
	Gelb/Grün	PRESET-Funktion erfolgreich beendet.
F	Rot	Beim Betrieb des SCALANCE W786 ist ein Fehler aufgetreten.
	Rot blinkend	Bereit zum Firmware-Laden. Das Gerät wurde entweder mit dem Reset-Taster angehalten oder im Gerät ist eine fehlerhafte Firmware vorhanden.

Hinweis

Wenn beim Anlauf die LED für das WLAN-Interface nicht grün wird, obwohl es aktiviert ist, so ist das Interface nicht betriebsbereit (Interface nicht initialisiert).

Das kann insbesondere daran liegen, dass bei Inbetriebnahme der SCALANCE W78x Produkte unter dem Gefrierpunkt (Umgebungstemperatur) eine Wartezeit bis zu 15 Minuten auftreten kann. Das Gerät ist bei der spezifizierten Umgebungstemperatur betriebsbereit, sobald die LED für das WLAN-Interface grün anzeigt.

2.5 C-PLUG

Konfigurationsinformation im C-PLUG

Der C-PLUG dient dazu, im Fall eines Geräteaustausches die Konfiguration des alten Geräts auf das Neugerät zu übertragen. Bei Start des neuen Geräts mit dem C-PLUG läuft dieses dann automatisch exakt mit der Konfiguration des alten Gerätes an. Ein Ausnahmefall kann die IP-Konfiguration darstellen, wenn sie per DHCP eingestellt wird und der DHCP-Server nicht entsprechend umkonfiguriert wurde.

Eine Nachkonfiguration ist erforderlich, wenn Sie WDS oder bei Geräten mit mehr als einer WLAN-Schnittstelle Redundanz nutzen und dabei die MAC-Adressen und nicht die sysNamen benutzen. Diese Funktionen basieren dann auf der MAC-Adresse, die sich bei einem Gerätetausch zwangsläufig ändert.

Hinweis

Im Bezug auf den C-PLUG arbeiten SCALANCE W-700-Geräte in zwei Modi:

- **Ohne C-PLUG**
  Das Gerät speichert die Konfiguration auf dem internen Speicher. Dieser Modus ist aktiv wenn kein C-PLUG gesteckt ist.
- **Mit C-PLUG**
  Die Konfiguration, die auf dem C-PLUG gespeichert ist, wird über die Benutzerschnittstellen angezeigt. Der interne Speicher wird in diesem Modus weder gelesen noch beschrieben. Bei Änderungen der Konfiguration speichert das Gerät die Konfiguration direkt auf dem C-PLUG. Dieser Modus ist aktiv, sobald ein C-PLUG gesteckt ist. Sobald das Gerät mit gestecktem C-PLUG gestartet wird, läuft der SCALANCE W-700 mit den Konfigurationsdaten auf dem C-PLUG an.

2.6 Reset-Taster

Funktionen des Reset-Tasters

Der Reset-Taster befindet sich unter der Gehäuseabdeckung neben den Anschlussbuchsen für die externen Antennen:

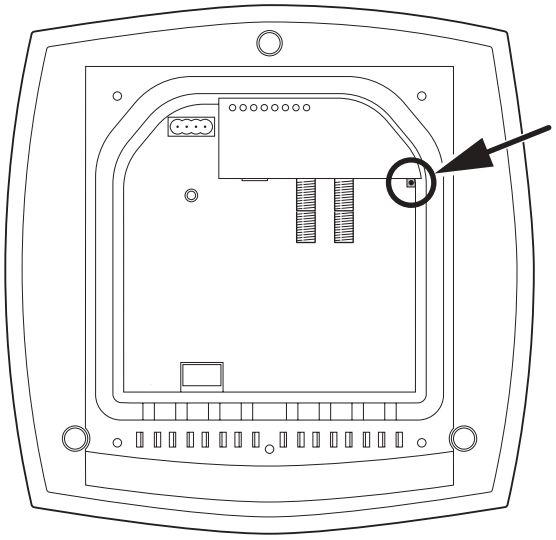


Bild 2-8 Position des Reset-Tasters bei abgenommenem Gehäusedeckel

Der Reset-Taster hat folgende Funktionen:

- **Neustart des Geräts**

  Um einen Neustart des Geräts durchzuführen, drücken Sie den Reset-Taster.

- **Laden einer neuen Firmware**

  Falls das reguläre Vorgehen über den Menüpunkt Load & Save des Web Based Managements nicht erfolgreich abgeschlossen wurde, kann der Reset-Taster zum Laden einer neuen Firmware genutzt werden. Dieser Fall kann eintreten, wenn es während des regulären Firmware-Updates zu einem Spannungsausfall kam.

- **Wiederherstellen der Default Parameter (Auslieferungszustand, Factory default)**
- **Übernahme der Konfigurationsdaten aus dem PRESET-PLUG.**

2.7 Biologische Verträglichkeit

Elektromagnetische Felder und Gesundheit

Hinsichtlich der Frage, ob elektromagnetische Felder (zum Beispiel im Zusammenhang mit Industrial Wireless LAN) die menschliche Gesundheit gefährden können, verweisen wir auf eine Publikation der BITKOM (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.), Stand Dezember 2003:

"Für WLAN-Geräte gelten die gleichen Vorschriften zum Schutz vor gesundheitlichen Beeinträchtigungen wie für alle anderen Funkanwendungen auch. Diese Vorschriften beruhen auf den Schutzkonzepten der ICNIRP[1] bzw. der entsprechenden EU-Ratsempfehlung.

Die unabhängige deutsche Strahlenschutzkommission (SSK) hat im Auftrag des BMU (Bundesministeriums für Umwelt) den Stand der Wissenschaft hinsichtlich möglicher Gefahren - thermisch und nicht thermisch - durch elektromagnetische Felder ermittelt und äußert sich wie folgt[2]:

'Die SSK kommt zu dem Schluss, dass auch nach der Bewertung der neueren wissenschaftlichen Literatur keine neuen wissenschaftlichen Erkenntnisse im Hinblick auf nachgewiesene Gesundheitsbeeinträchtigungen vorliegen, die Zweifel an der wissenschaftlichen Bewertung aufkommen lassen, die den Schutzkonzepten der ICNIRP bzw. der EU-Ratsempfehlung zugrunde liegt.'

Darüber hinaus stellt die SSK fest, dass unterhalb der bestehenden Grenzwerte auch kein wissenschaftlicher Verdacht auf gesundheitliche Risiken besteht.

Diese Bewertung stimmt mit denen anderer nationaler und internationaler wissenschaftlicher Kommissionen sowie der WHO (`www.who.int/emf`) überein.

Dementsprechend und angesichts der Tatsache, dass WLAN-Geräte die wissenschaftlich fundierten Grenzwerte deutlich unterschreiten, gehen von den elektromagnetischen Feldern von WLAN-Produkten keine gesundheitlichen Gefahren aus.

[1] Internationale Kommission zum Schutz vor Nicht-Ionisierender Strahlung

[2] 'Grenzwerte und Vorsorgemaßnahmen zum Schutz der Bevölkerung vor elektromagnetischen Feldern', Empfehlung der Strahlenschutzkommission mit wissenschaftlicher Begründung, Heft 29, 2001."

Weitere Informationen zu diesem Thema finden Sie im Internet unter folgender URL:

`www.bitkom.org`

Montage

3

3.1 Demontage / Montage des Gehäusedeckels

Wann müssen Sie den Gehäusedeckel demontieren?

Folgende Tätigkeiten können Sie nur bei abgenommenem Gehäusedeckel durchführen:

- Sie wollen den SCALANCE W786 an eine Wand oder auf das optional erhältliche Halteblech aufschrauben.
- Sie wollen Leitungen für die Spannungsversorgung, für Ethernet oder für externe Antennen an den SCALANCE W786 anschließen.
- Sie wollen einen C-PLUG in das Gerät einsetzen oder einen vorhandenen C-PLUG austauschen.
- Sie wollen den Reset-Taster benutzen.

Demontage des Gehäusedeckels

⚠ WARNUNG

Lebensgefahr durch Netzspannung

Nach der Demontage des Gehäusedeckels besteht die Gefahr, spannungsführende Teile zu berühren.

Führen Sie die Demontage des Gehäusedeckels erst durch, nachdem Sie die Stromversorgung des SCALANCE W786 abgeschaltet haben.

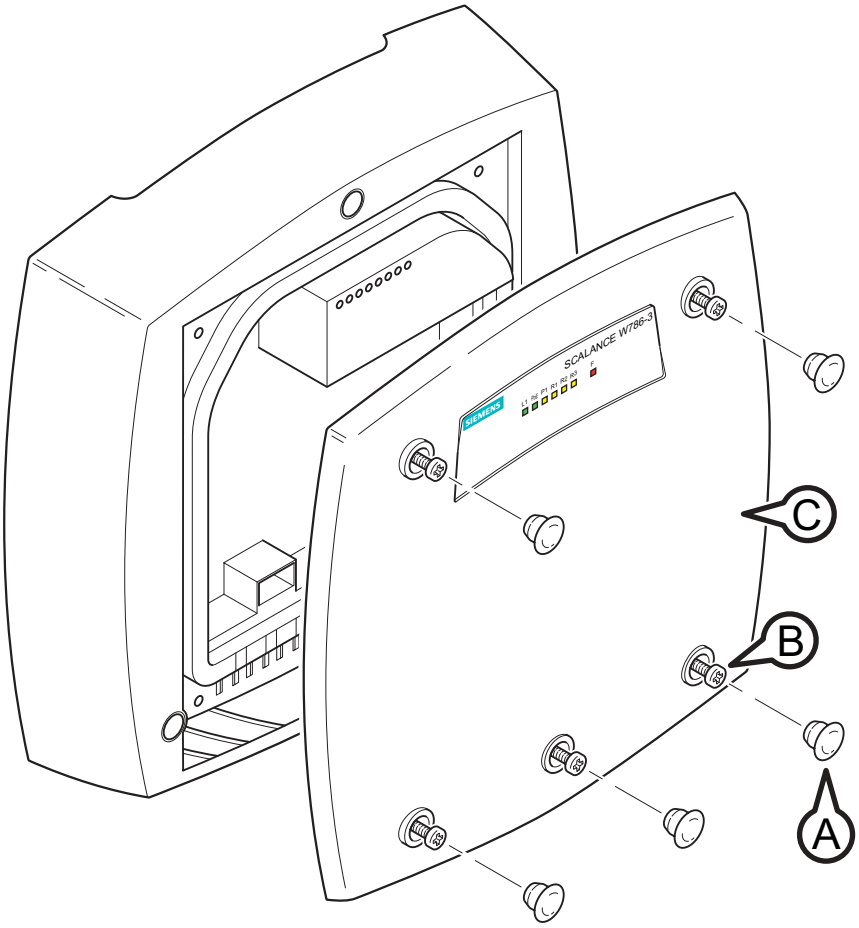


Bild 3-1 Deckeldemontage
A Verschlusskappe
B Deckelverschraubung
C Gehäusedeckel

Führen Sie folgende Schritte durch, um den Gehäusedeckel zu demontieren:

1. Nehmen Sie die Verschlusskappen aus dem Gehäusedeckel (Position **A** in der vorangegangenen Abbildung)
2. Lösen Sie die Deckelverschraubung (Position **B** in der vorangegangenen Abbildung).

Hinweis

Auch nach dem Lösen verbleiben diese Schrauben im Gehäusedeckel (Verliersicherung). Versuchen Sie deshalb nicht, diese Schrauben gewaltsam aus dem Gehäusedeckel zu entfernen, weil dadurch der Gehäusedeckel beschädigt wird!

3. Nehmen Sie den Gehäusedeckel mit den darin verbliebenen Schrauben ab (Position **C** in der vorangegangenen Abbildung).

Montage des Gehäusedeckels

Die Montage des Gehäusedeckels erfolgt in umgekehrter Reihenfolge wie die Demontage. Anzugsmoment für die Deckelverschraubung 1,8 Nm.

3.2 Verlegung der Leitungen

Verlegung der Leitungen vor der Montage

Bevor Sie einen SCALANCE W786 an eine Wand oder auf das optional erhältliche Halteblech aufschrauben, müssen Sie die Leitungen für die Spannungsversorgung, für Ethernet und gegebenenfalls für die externen Antennen verlegen. Es gibt folgende Möglichkeiten:

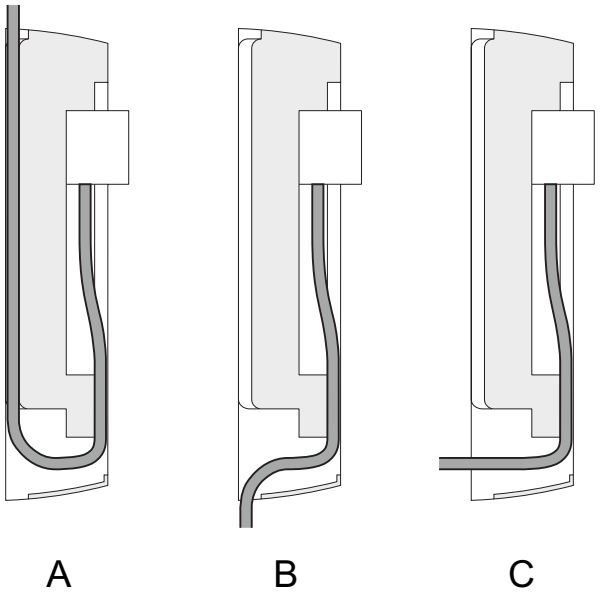


Bild 3-2 Seitenansicht eines SCALANCE W786 mit Leitungszuführung aus verschiedenen Richtungen

- Die Leitungen werden von oben eingebracht (Position **A** in der vorangegangenen Abbildung). Das Gehäuse des SCALANCE W786 verfügt an der Oberseite über eine entsprechende Aussparung.
- Die Leitungen werden von unten eingebracht (Position **B** in der vorangegangenen Abbildung). Auch an der Gehäuseunterseite gibt es für diesen Zweck eine Aussparung.
- Leitungszuführung durch eine Wand hinter dem SCALANCE W786 (Position **C** in der vorangegangenen Abbildung). In diesem Fall müssen Sie den SCALANCE W786 so montieren, dass sich der Wanddurchbruch über der Unterkante des Geräts befindet.

Verlegung von Lichtwellenleitern

Lichtwellenleiter haben einen minimal zulässigen Biegeradius . Weder bei der Montage noch im Betrieb darf dieser Radius unterschritten werden, weil der Lichtwellenleiter sonst zerstört wird.

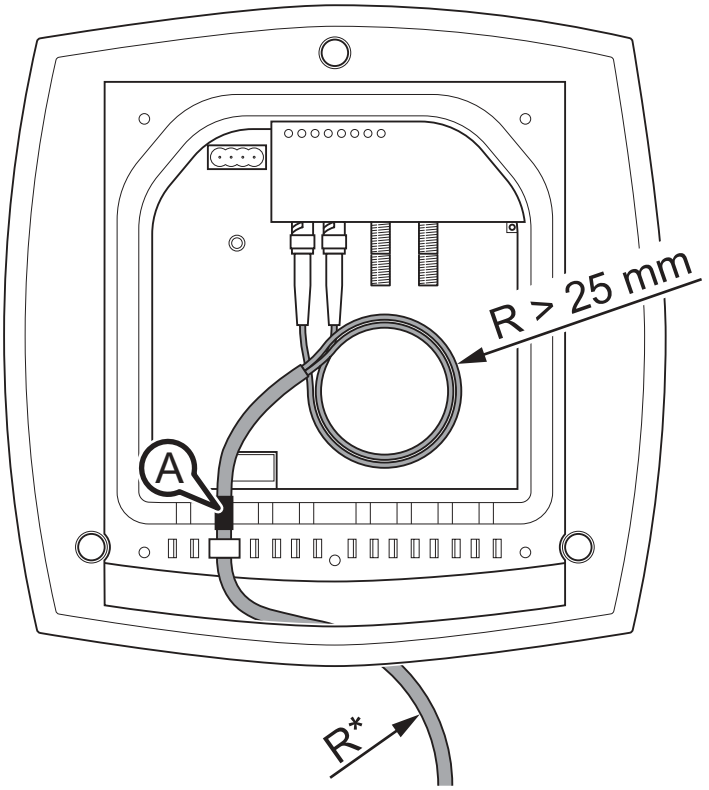


Bild 3-3 Verlegen einer FO-Leitung

Benutzen Sie für die FO-Leitung den zweiten Dichtungsdurchbruch von links. Die Kabelführung ist in der vorangegangenen Abbildung dargestellt. Für die einzelnen Adern unmittelbar hinter der Steckerverbindung beträgt der minimale Biegeradius 25 mm. Den minimal zulässigen Biegeradius R* für die ummantelte Leitung entnehmen Sie der Spezifikation der verwendeten Leitung. Keinesfalls darf der Lichtwellenleiter scharf abgeknickt werden, um ihn hinter dem Gehäuse zu verlegen.

Lichtwellenleiter dürfen nur mit der Dichtungsklebefolie (Position **A** in der vorangegangenen Abbildung) in der Gehäusedichtung verlegt werden. Detailinformationen dazu finden Sie im Kapitel "Anschließen der Leitungen".

Masseanschluss

⚠ WARNUNG

Für den sicheren Betrieb des SCALANCE W786 ist es unbedingt notwendig, den Masseanschluss mit einer entsprechenden Leitung zu versehen. Verwenden Sie den SCALANCE W786 nicht ohne angeschlossene Masseleitung.

Der Masseanschluss befindet sich auf der Gehäuserückseite (Gewinde M4). Sie müssen die Masseleitung anschließen, bevor Sie den SCALANCE W786 an eine Wand oder das optional erhältliche Halteblech anbringen. Nach der Montage eines SCALANCE W786 ist dieser Anschluss nicht mehr zugänglich.

Legen Sie die mitgelieferte Schneidscheibe direkt auf die Gehäuserückseite, bevor Sie die Masseleitung aufschrauben. Nur so stellen Sie sicher, dass ein einwandfreier Kontakt zur aufgeschraubten Leitung hergestellt wird.

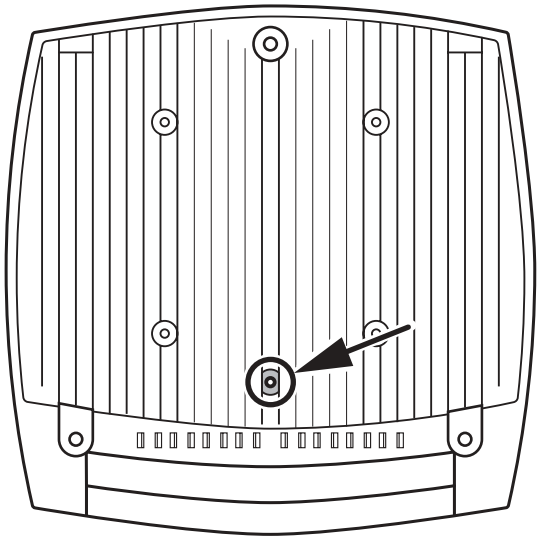


Bild 3-4 Masseanschluss auf der Rückseite des SCALANCE W786

3.3 Montage ohne Adapter (Nur Wandmontage)

Bohrbild

Die Lage der Bohrungen für die Wandmontage des SCALANCE W786 ist in der folgenden Abbildung dargestellt:

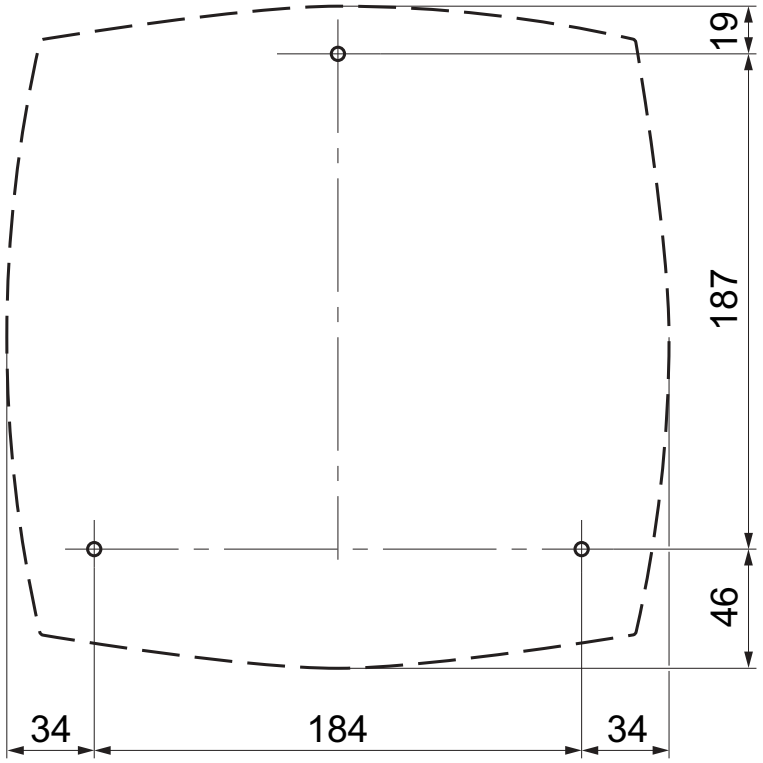


Bild 3-5 Bohrbild für die Wandmontage eines SCALANCE W786

Vorgehensweise

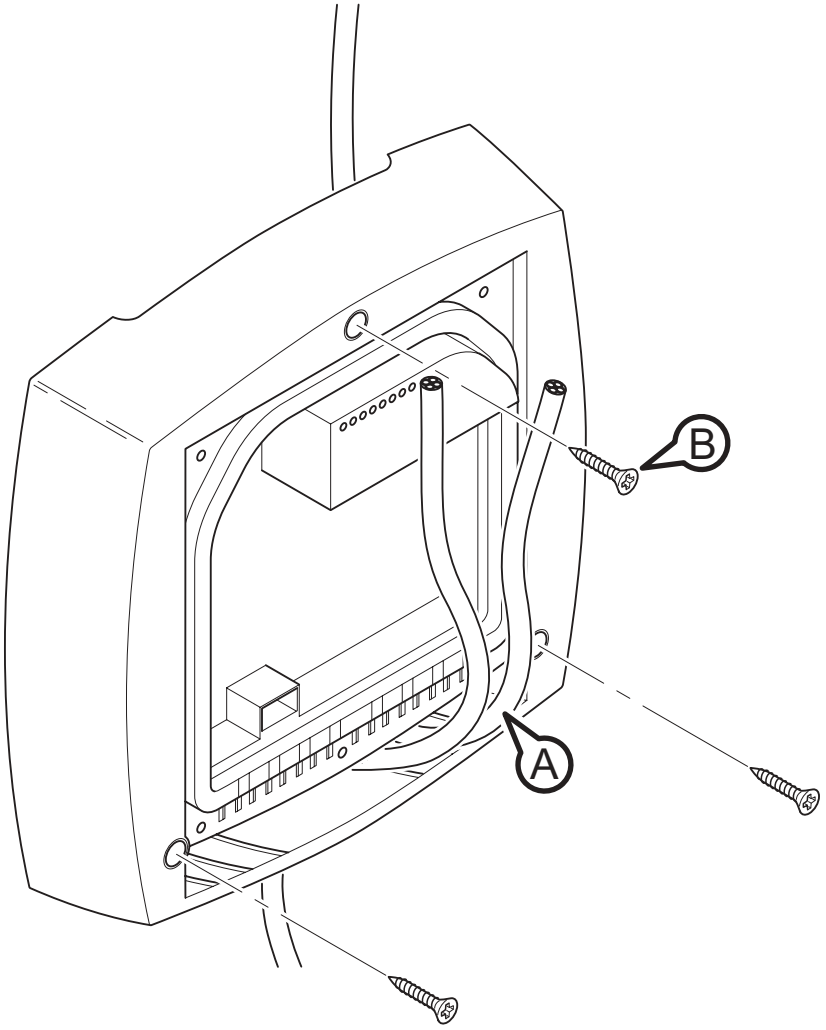


Bild 3-6 Wandmontage eines SCALANCE W786

Führen Sie folgende Schritte durch, um einen SCALANCE W786 auf eine Wand aufzuschrauben:

1. Führen Sie die Leitungen in das Gehäuse des SCALANCE W786 ein (Position **A** in der vorangegangenen Abbildung). Beachten Sie dabei die Informationen im Kapitel "Verlegung der Leitungen".
2. Befestigen Sie den SCALANCE W786 mit drei Schrauben auf der Wand (Position **B** in der vorangegangenen Abbildung). Die Schrauben sind nicht im Lieferumfang enthalten. Art und Länge der Schrauben hängen von der Beschaffenheit der Wand ab.
   Art der Schrauben:
   - für Holzwände: Holzschraube 4 x 30 mm
   - für Betonwände: 4 x 50mm mit 5 mm Betondübel
   - für Metallwände: M4 x 25 mm mit Maschinengewinde in der Wand

Option: Gewindebohrungen auf der Gehäuserückseite

In sehr dünnen Wänden können häufig keine Dübel für die Verschraubung eingebracht werden. Um auch in diesen Fällen eine Wandmontage zu ermöglichen, befinden sich auf der Gehäuserückseite des SCALANCE W786 vier Gewindebohrungen M4. Das Bohrbild ist ein Quadrat mit der Seitenlänge 100 mm. Sie können das Gerät also auch über Durchgangsbohrungen in der Wand anbringen.

Ermitteln Sie die Länge der dafür notwendigen M4-Schrauben wie folgt:

Schraubenlänge = Wandstärke + 7 mm

3.4 Montage mit Halteblech

3.4.1 Wandmontage des Halteblechs

Bohrbild

Die Lage der Bohrungen für die Wandmontage des Halteblechs ist in der folgenden Abbildung dargestellt:

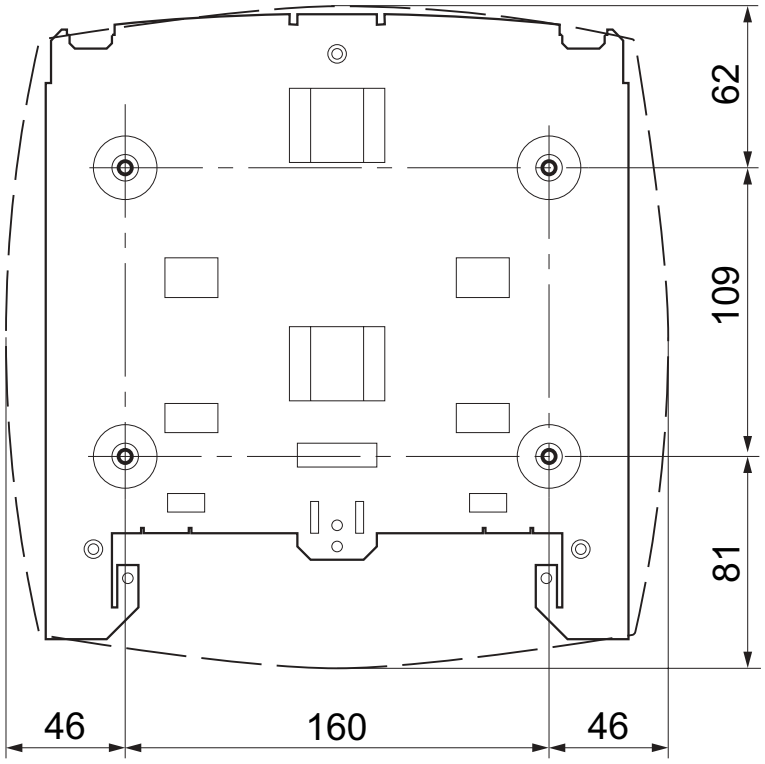


Bild 3-7 Bohrbild für die Wandmontage des Halteblechs

Vorgehensweise

Befestigen Sie das Halteblech mit vier Schrauben auf der Wand. Die Schrauben sind nicht im Lieferumfang enthalten. Art und Länge der Schrauben hängen von der Beschaffenheit der Wand ab.
Art des Schrauben:

- für Holzwände: Holzschraube 4 x 30 mm
- für Betonwände: 4 x 50mm mit 5 mm Betondübel
- für Metallwände: M4 x 25 mm mit Maschinengewinde in der Wand

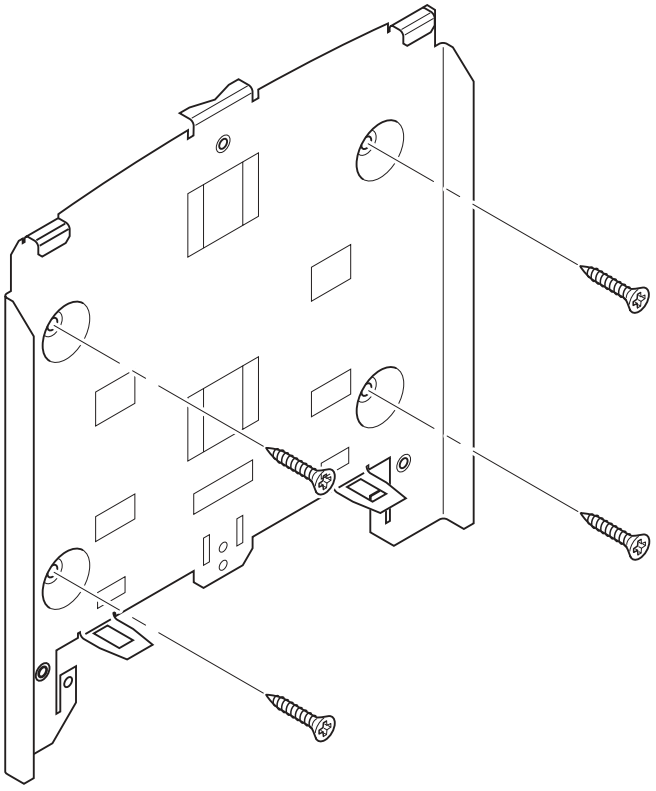


Bild 3-8 Wandmontage des Halteblechs für den SCALANCE W786

3.4.2 Aufschrauben des Abdeckblechs für die Kabelzuführung auf das Halteblech

Schutz der Kabelzuführung gegen starkes Strahlwasser

Die Verkabelung eine SCALANCE W786 wird auf der Gehäuserückseite aus dem Gerät herausgeführt. Die Gehäuseabdichtung kann ihre Funktion nur erfüllen, wenn sie nicht direkt starkem Strahlwasser ausgesetzt ist. Bei Wandmontage ist diese Voraussetzung ohne weitere Maßnahmen gegeben. Bei allen anderen Montagearten außer der Montage auf einer S7-300-Profilschiene müssen Sie ein zusätzliches Abdeckblech auf das Halteblech aufschrauben.

⚠ WARNUNG

Lebensgefahr durch Netzspannung

Wenn die Kabelzuführung auf der Gehäuserückseite starkem Strahlwasser ausgesetzt ist, kann Wasser in das Gerät eindringen und eine leitende Verbindung zu Netzspannung herstellen. Es besteht die Gefahr eines Stromschlags.

Verwenden Sie unbedingt das Abdeckblech für die Kabelzuführung, wenn Sie den SCALANCE W786 nicht auf eine Wand aufschrauben.

Vorgehensweise

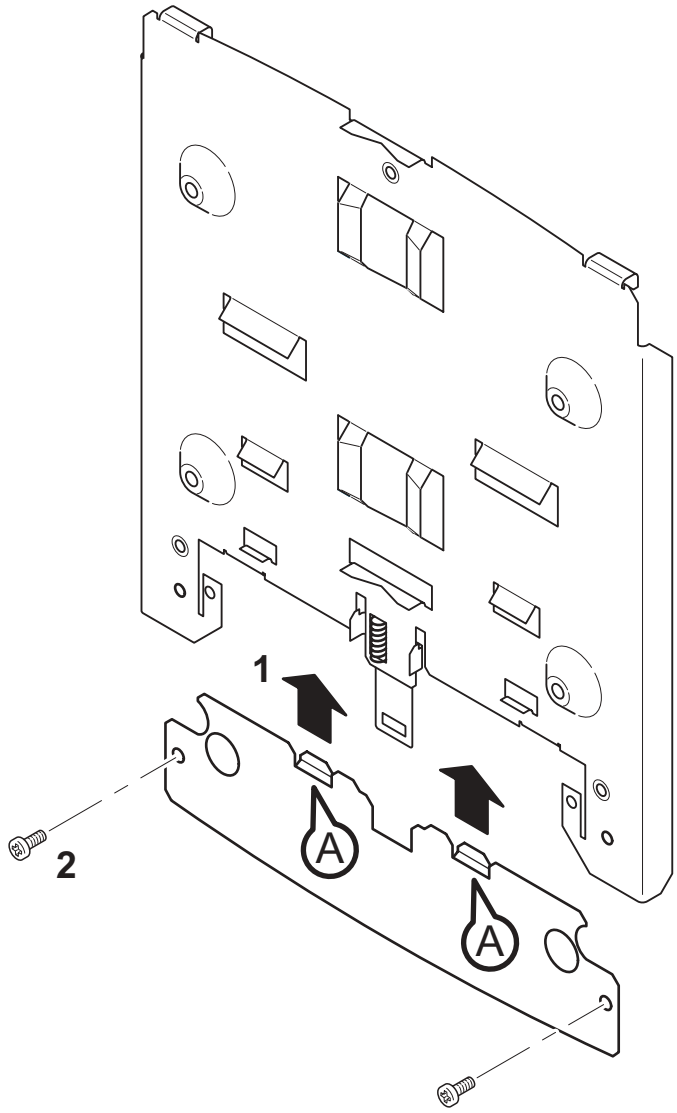


Bild 3-9 Aufstecken und Aufschrauben des Abdeckblechs für die Kabelzuführung

Führen Sie folgende Schritte durch, um das Abdeckblech für die Kabelzuführung auf das Halteblech aufzuschrauben:

1. Stecken Sie das Abdeckblech von unten auf das Halteblech, bis die beiden Laschen (Position **A** in der vorangegangenen Abbildung) in die Unterkante des Halteblechs eingreifen.
2. Befestigen Sie das Abdeckblech mit zwei M4-Schrauben auf dem Halteblech. Die Schrauben sind im Lieferumfang des Montagesatzes enthalten.

3.4.3 Montage des Halteblechs auf einer S7-300-Profilschiene

Vorgehensweise

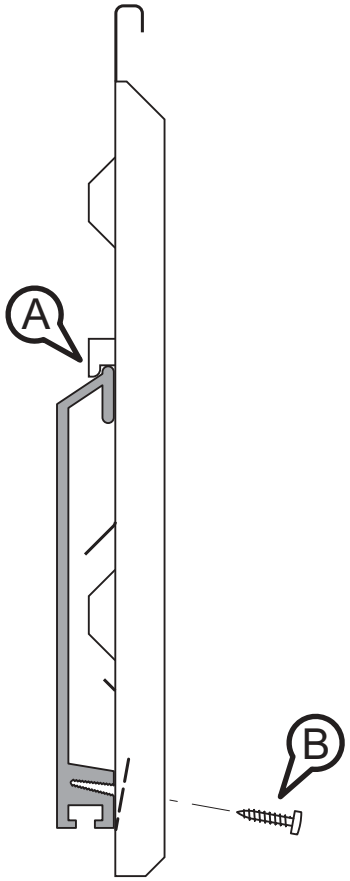


Bild 3-10 Seitenansicht eines Halteblechs auf einer S7-300-Profilschiene

Führen Sie folgende Schritte durch, um das Halteblech auf einer S7-300-Profilschiene zu montieren:

1. Setzen Sie das Halteblech mit den beiden vorstehenden Haken auf die Oberkante der S7-300-Profilschiene (Position **A** in der vorangegangenen Abbildung).
2. Das Halteblech verfügt am unteren Ende über zwei Laschen mit Bohrungen. Verschrauben Sie diese Laschen mit der S7-300-Profilschiene (Position **B** in der vorangegangenen Abbildung). Die dafür notwendigen Schrauben gehören zum Lieferumfang des Halteblechs.

3.4.4 Montage des Halteblechs auf einer Hutschiene

Vorgehensweise

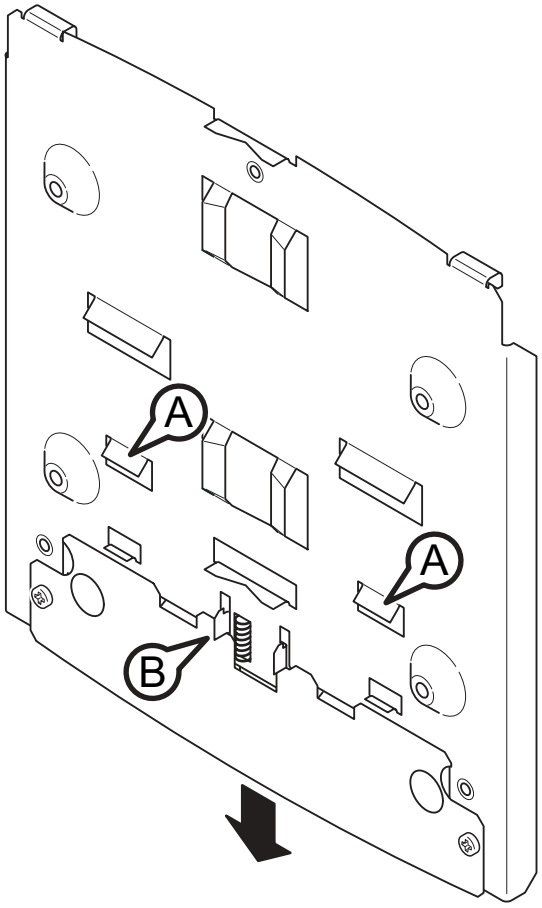


Bild 3-11 Halteblech mit Befestigungselementen für die Hutschienenmontage

Führen Sie folgende Schritte durch, um das Halteblech auf einer Hutschiene zu montieren:

1. Setzen Sie das Halteblech mit den beiden Montagelaschen (Position A in der vorangegangenen Abbildung) auf die Oberkante der Hutschiene.
2. Ziehen Sie den Hutschienenschieber (Position B in der vorangegangenen Abbildung) nach unten und drücken Sie das Halteblech gegen die Hutschiene, bis der Hutschienenschieber dort einrastet.

3.4.5 Mastmontage des Halteblechs

Vorgehensweise

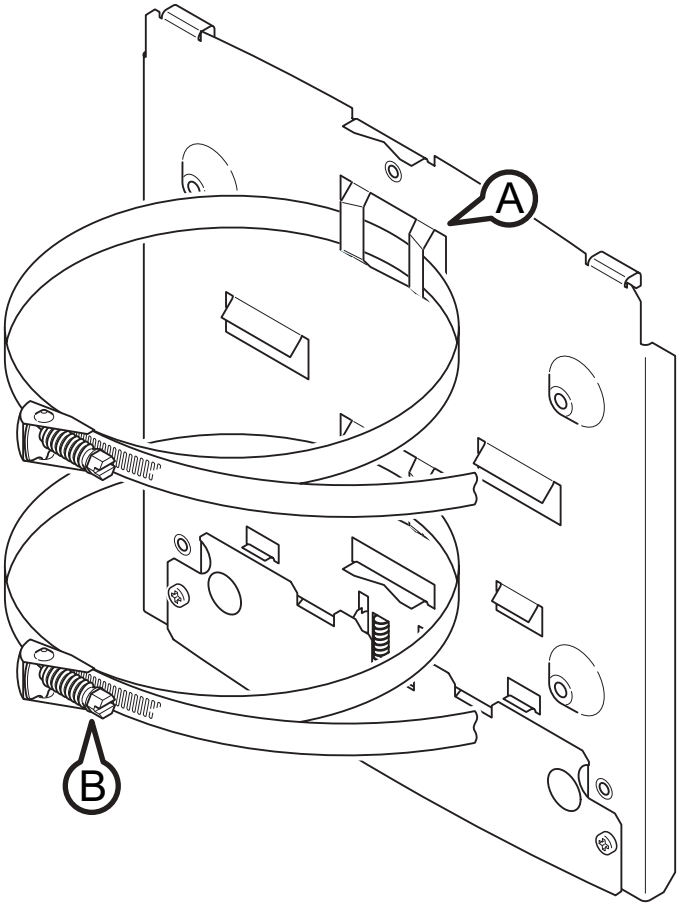


Bild 3-12 Halteblech mit Befestigungselementen für die Mastmontage

Führen Sie folgende Schritte durch, um das Halteblech an einem Mast zu montieren:

1. Führen Sie die Befestigungsbänder durch die Aufnahmen des Halteblechs (Position **A** in der vorangegangenen Abbildung).
2. Legen Sie die Befestigungsbänder an der gewünschten Position um den Mast.
3. Führen Sie das freie Ende eines Befestigungsbandes durch den Schnellverschluss. Sie können die Spannschraube (Position **B** in der vorangegangenen Abbildung) zur Seite schwenken, um den Durchmesser eines Befestigungsbandes an den Mastdurchmesser anzupassen.
4. Drücken Sie die Spannschraube gegen das Befestigungsband und ziehen Sie die Spannschraube an, Anzugsmoment 4,5 Nm.

3.4.6 Montage/Demontage des SCALANCE W786 auf ein Halteblech

Vorgehensweise bei der Montage

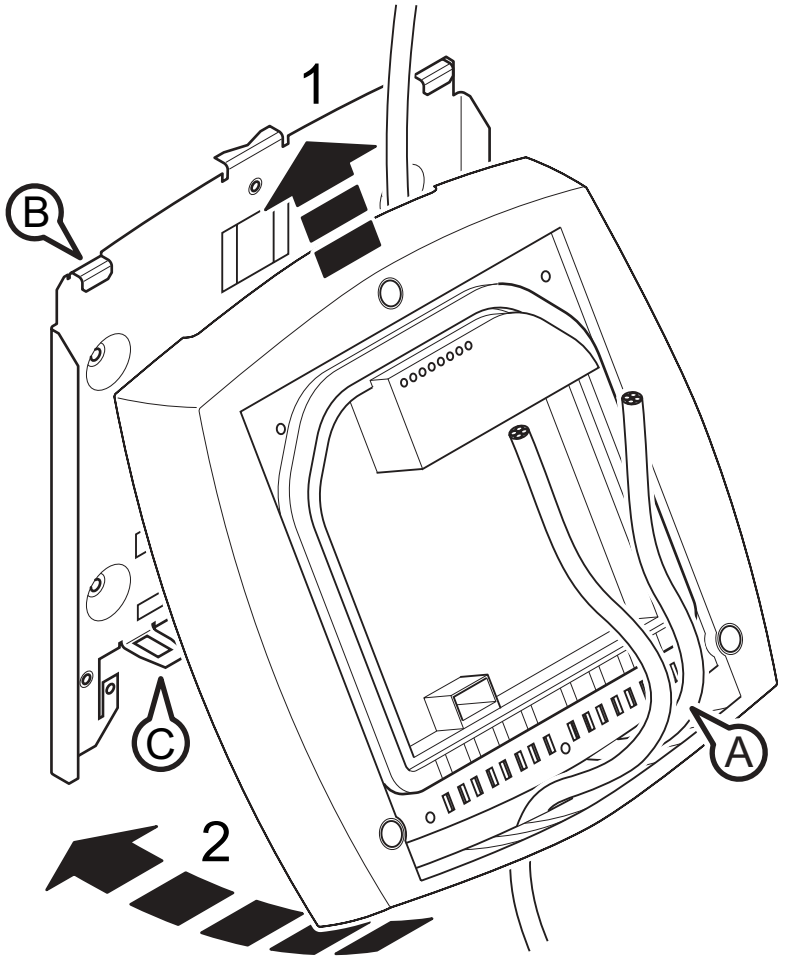


Bild 3-13 Aufstecken eines SCALANCE W786 auf ein Halteblech

Führen Sie folgende Schritte durch, um einen SALANCE W786 auf einem Halteblech zu montieren:

1. Führen Sie die Leitungen in das Gehäuse des SCALANCE W786 ein (Position **A** in der vorangegangenen Abbildung). Beachten Sie dabei die Informationen im Kapitel "Verlegung der Leitungen".
2. Schieben Sie den SCALANCE W786 mit der Oberkante der Gehäuserückseite unter die beiden Aufnahmelaschen des Halteblechs (Position **B** in der vorangegangenen Abbildung).
3. Schwenken Sie den SCALANCE W786, bis er in den Ausklinkungen an der Unterkante des Halteblechs (Position **C** in der vorangegangenen Abbildung) einrastet.

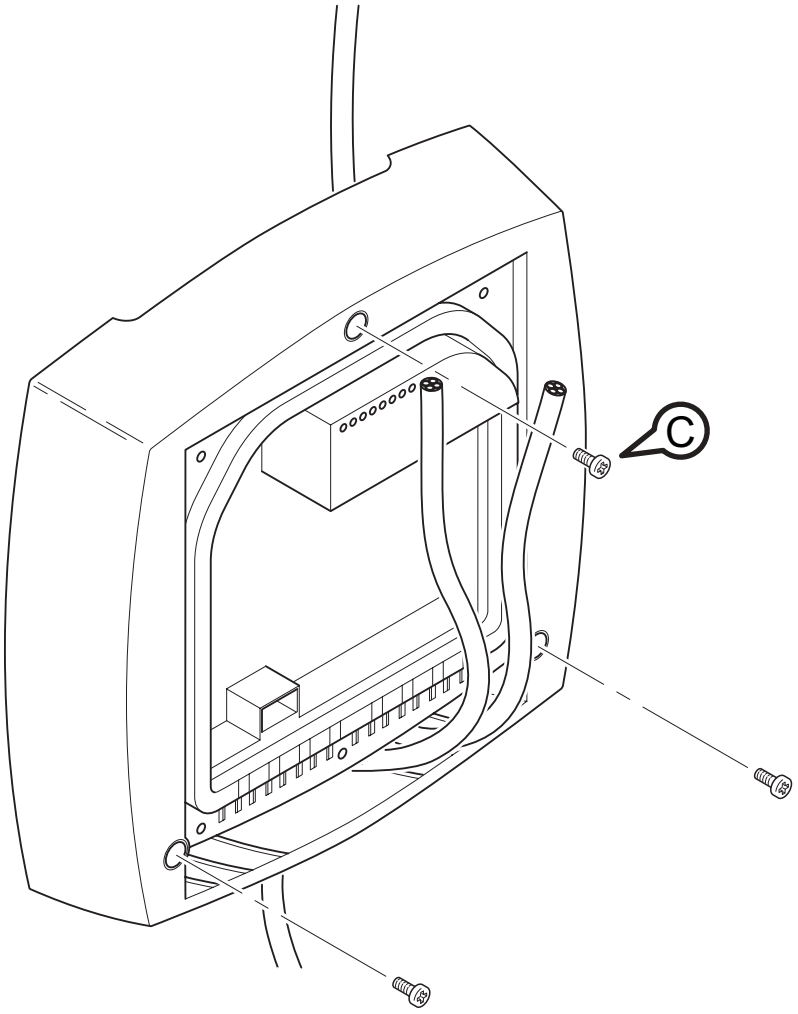


Bild 3-14 Aufschrauben eines SCALANCE W786 auf einem Halteblech

4. Verschrauben Sie den SCALANCE W786 mit den drei M4-Schrauben, die zum Lieferumfang des Halteblechs gehören (Position **D** in der vorangegangenen Abbildung), Anzugsmoment 1,8 Nm.

Vorgehensweise bei der Demontage

Führen Sie folgende Schritte durch, um einen SALANCE W786 vom Halteblech zu demontieren:

1. Lösen Sie die Verschraubung von SCALANCE W786 und Halteblech.
2. Drücken Sie die beiden Laschen an der Unterkante des Halteblechs (Position **C** in der ersten Abbildung dieses Kapitels) nach unten (z. B. mit Schraubendrehern) und lösen Sie den SCALANCE W786 aus den Ausklinkungen.
3. Schwenken Sie die Unterkante des SCALANCE W786 nach vorne und lösen Sie ihn aus den beiden Aufnahmelaschen des Halteblechs (Position **B** in der ersten Abbildung dieses Kapitels).

Anschließen

4

4.1 Blitzschutz, Versorgungsspannung und Erdung

Hinweise zum Blitzschutz

⚠ WARNUNG

Lebensgefahr durch Blitzschlag

Antennen im Außenbereich müssen sich im Fangbereich eines Blitzableiters befinden. Stellen Sie sicher, dass für alle von außen eingeführten leitfähigen Systeme die Möglichkeit eines Blitzschutz-Potenzialausgleichs gegeben ist.

Beachten Sie bei der Umsetzung Ihres Blitzschutzkonzepts unbedingt die Anforderungen der Normen VDE 0182 bzw. IEC 62305.

Ein geeignetes Blitzschutzelement ist im Zubehörprogramm von SIMATIC NET Industrial WLAN verfügbar:

Blitzschutzelement LP798-1N (Bestell-Nr. 6GK5798-2LP00-2AA6)

⚠ WARNUNG

Lebensgefahr durch Blitzschlag

Der Einbau des genannten Blitzschutzelements zwischen einer Antenne und einem SCALANCE W-700 stellt noch keinen ausreichenden Schutz gegen Blitzeinschlag dar. Das Blitzschutzelement LP798-1N ist nur im Rahmen eines umfassenden Blitzschutzkonzepts funktionsfähig. Wenden Sie sich an einen qualifizierten Fachbetrieb, wenn Sie dazu Fragen haben.

Hinweis

Die Anforderungen nach EN61000-4-5, Surge Prüfung auf Spannungsversorgungsleitungen, werden bei DC 12 - 24 V und DC 48 V nur erfüllt bei Einsatz eines Blitzductors:

DC 12 - 24 V: VT AD 24V Art. Nr. 918 402

DC 48 V: Art.-Nr. 919 545 und 919 506 (Halter)

Hersteller: DEHN+SÖHNE GmbH+Co.KG, Hans Dehn Str. 1, Postfach 1640, D-92306 Neumarkt

Sicherheitskleinspannung

⚠ WARNUNG

Lebensgefahr durch Überspannung, Brandgefahr

Die Geräte SCALANCE W-700 sind für den Betrieb mit einer direkt anschließbaren Sicherheitskleinspannung oder mit den als Zubehör erhältlichen Stromversorgungsadaptern (nur für das Gerät SCALANCE W786-xPRO verfügbar) ausgelegt. Deshalb dürfen an die Versorgungsanschlüsse nur Sicherheitskleinspannungen (SELV) mit begrenzter Leistung (LPS) nach IEC950/EN60950/VDE0805 angeschlossen werden (Ausnahme: Stromversorgungsadapter für AC 110 - 230 V für den SCALANCE W786-xPRO).

Das Netzteil für die Versorgung eines SCALANCE W-700 muss NEC Class 2 (Anforderungen der Klasse 2 für Stromversorgungen der "National Electrical Code, table 11 (b)") oder SELV mit LPS (Limited Power Source) EN 60950-1 entsprechen. Bei einem Aufbau mit redundanter Spannungsversorgung (zwei getrennte Spannungsversorgungen) müssen beide Spannungsversorgungen diese Anforderungen erfüllen.

Ausnahmen:

- Die Versorgung durch PELV (entsprechend DIN VDE 0100-410 bzw. IEC 60364-4-41) ist ebenfalls zulässig, sofern die erzeugte Nennspannung die Spannungsgrenzen AC 25 V oder DC 60 V nicht überschreitet.

Erdung

VORSICHT

Beschädigung des Geräts durch Potentialunterschied

Um eine Beeinflussung durch elektromagnetische Störungen zu vermeiden, sollte das Gerät geerdet montiert werden. Zwischen folgenden Teilen darf kein Potenzialunterschied bestehen, da sonst das Gerät oder angeschlossene weitere Geräte möglicherweise zerstört werden:

- Gehäuse des SCALANCE W-700 und dem Erdpotential der Antenne.
- Gehäuse des SCALANCE W-700 und dem Erdpotential eines über Ethernet angeschlossenen Gerätes.
- Gehäuse des SCALANCE W-700 und der Schirmauflage des angeschlossenen Ethernet-Kabels.

Legen Sie beide Erdungen auf den gleichen Fundamenterder oder verwenden Sie eine Potenzialausgleichsleitung.

Unterbrechung der Stromversorgung

VORSICHT
Beschädigung der Ethernet-Schnittstelle Wiederholtes schnelles Ziehen und Stecken des Ethernet-Kabels mit Power-over-Ethernet-Speisung bei gleichzeitiger redundanter Stromversorgung kann zur Beschädigung der Ethernet-Schnittstelle führen. Vermeiden Sie wiederholtes Ziehen und Stecken des Ethernet-Kabels bei Power-over-Ethernet-Speisung und redundanter Stromversorgung.

4.2 Geeignete Leitungen und Antennen für den SCALANCE W786

Spezifikation der Leitungen

Die folgende Tabelle führt auf, welche Anforderungen eine Leitung abhängig vom Einsatzfall erfüllen muss.

Einsatzfall	Spezifikation
Direkteinspeisung DC 48 V	• Runder Kabelquerschnitt mit 6 bis 8 mm Durchmesser. • Zulässige Zugkraft mindestens 100 N. • UL Listung: Type PLTC oder ITC
Stromversorgungsadapter DC 12 - 24 V	• Runder Kabelquerschnitt mit 6 bis 8 mm Durchmesser. • Zulässige Zugkraft mindestens 100 N. • UL Listung: Type PLTC oder ITC
Stromsversorgungsadapter AC 110 - 230 V	• Runder Kabelquerschnitt mit 6 bis 8 mm Durchmesser. • Dreiadriges Kabel mit 0,5 - 1,5 mm^2 Querschnitt der Einzeladern. • Zulässige Zugkraft mindestens 100 N.
Ethernet	IE FC TP Standard Cable GP 2 x 2 (Type A) Best.-Nr. 6XV1 840-2AH10 IE TP Torsion Cable 2 x 2 (Type C) Best.-Nr. 6XV1 870-2F IE FC TP Trailing Cable 2 x 2 (Type C) Best.-Nr. 6XV1 840 3AH10 UL Listung: Type PLTC oder ITC (die drei genannten Typen besitzen diese Zulassung)
Lichtwellenleitung Multimode	FO Standard Cable GP Best.-Nr. 6XV1 873-2A Minimaler Biegeradius 65 mm. Detailinformationenen zu vorkonfektionierten Kabellängen und Steckern finden Sie im "Katalog IK PI".

Antennenanschluss: Anschlusskabel N-Connect/R-SMA

Zum direkten Anschluss einer Antenne an einen SCALANCE W-700 ist das N-Connect/R-SMA Male/Male Flexible Connection Cable als Zubehör lieferbar.

Länge in m	Bestellnummer
1	6XV1875-5CH10
2	6XV1875-5CH20
5	6XV1875-5CH50
10	6XV1875-5CN10

Antennenanschluss: Anschlusskabel N-Connect/ N-Connect

Zur Verbindung einer Antenne mit dem Blitzschutzelement LP798-1N ist das N-Connect/N-Connect Male/Male Flexible Connection Cable als Zubehör lieferbar.

Länge in m	Bestellnummer
1	6XV1875-5CH10
2	6XV1875-5CH20
5	6XV1875-5CH50
10	6XV1875-5CN10

Für IWLAN-Geräte, die sich in einem Schaltschrank befinden, gibt es eine Schaltschrankdurchführung mit entsprechenden Leitungen. Detailinformationen finden Sie im Katalog IK PI.

Antennen

Für die Verwendung mit einem SCALANCE W786-xPRO sind folgende Antennen freigegeben:

Typ	Eigenschaften	Bestell-Nr.
ANT795-6MN	Omniantenne 2,4 / 5GHz, Deckenmontage	6GK5795-6MN00-0AA6
ANT792-6MN	Omniantenne 2,4 GHz, Wandmontage	6GK5792-6MN00-0AA6
ANT793-6MN	Omniantenne 5 GHz, Wandmontage	6GK5793-6MN00-0AA6
ANT792-8DN	Richtantenne 2,4 GHz, Wandmontage	6GK5792-8DN00-0AA6
ANT793-8DN	Richtantenne 5 GHz, Wandmontage	6GK5793-8DN00-0AA6
ANT795-6DN	Richtantenne 2,4 / 5 GHz, Wandmontage	6GK5795-6DN00-0AA6
ANT792-4DN	RCoax-Antenne 2,4 GHz	6GK5792-4DN00-0AA6
ANT793-4MN	RCoax-Antenne 5 GHz	6GK5793-4MN00-0AA6

4.3 Anschließen der Leitungen

Vorgehenweise

⚠ WARNUNG

Lebensgefahr durch Netzspannung

Bei einem nicht einwandfrei abgedichteten Gehäuse besteht Lebensgefahr durch Netzspannung, wenn der SCALANCE W786 Spritzwasser oder Feuchtigkeit ausgesetzt ist. Beachten Sie unbedingt die folgenden Sicherheitsregeln.

- Schalten Sie die Leitung für die Stromversorgung vor dem Anschließen spannungslos.
- Die Abdichtung der Kabelzuführung des SCALANCE W786 ist nur bei Leitungen mit einem geeigneten Durchmesser und einer ausreichenden Zugfestigkeit sichergestellt. Verwenden Sie deshalb nur Leitungen, die den Spezifikationen im Kapitel "Leitungen für den SCALANCE W786" entsprechen. Montieren Sie beim Verlegen eines Lichtwellenleiters unbedingt die Dichtungsklebefolie, die zum Lieferumfang des SCALANCE W786 gehört.
- Umwickeln Sie niemals zu dünne Leitungen mit Isolierband, Klebeband oder einem anderen Material, um den geforderten Durchmesser zu erhalten. In diesem Fall können weder die Gehäusedichtung noch die Zugentlastungsklammern ihre Funktion erfüllen.
- Verschließen Sie alle nicht benutzten Durchbrüche in der Gehäusedichtung mit den Blindstopfen, die zum Lieferumfang des SCALANCE W786 gehören. Verwenden Sie dafür auf keinen Fall Dichtungsmasse oder eine anderes Material.

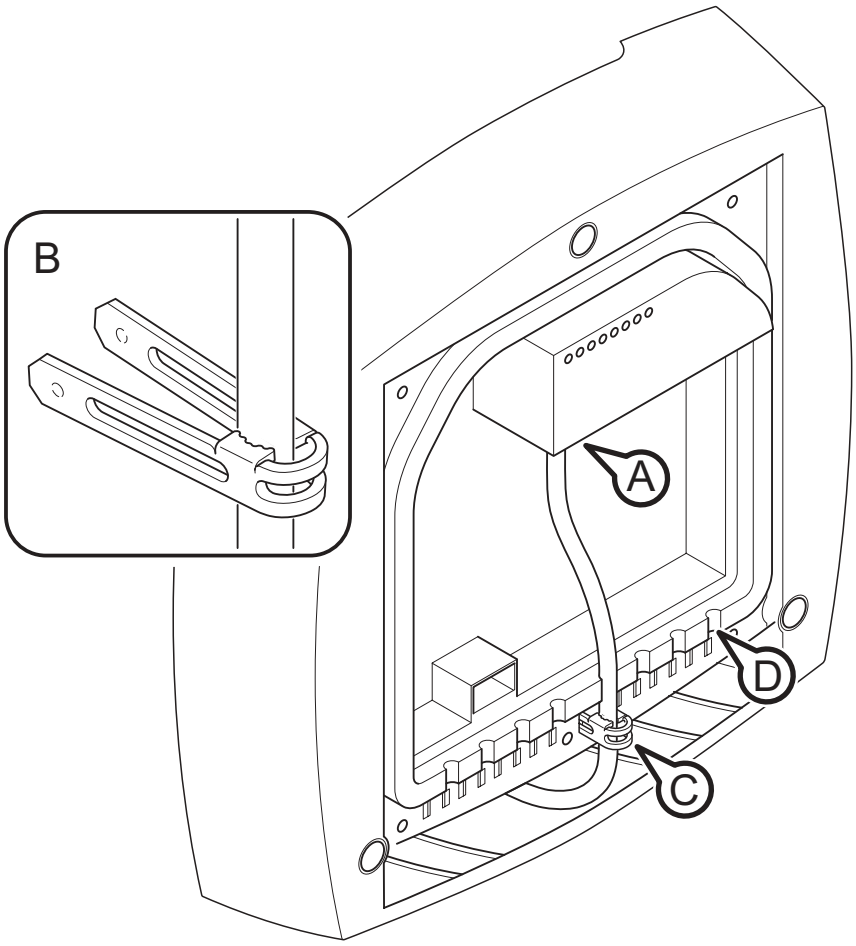


Bild 4-1 Anschließen einer Leitung und Anbringen der Zugentlastungsklammer

Führen Sie folgende Schritte durch, um Leitungen mit dem SCALANCE W786 zu verbinden:

1. Schließen Sie die Leitungen an den entsprechenden Kontakten an. (Position **A** in der vorangegangenen Abbildung) Es gibt folgende Möglichkeiten:
   - Leitungen, die bereits mit einem Stecker konfektioniert sind (Ethernet, Antennen), schließen Sie durch Einstecken in die entsprechende Buchse an. Antennenleitungen sichern Sie zusätzlich, indem Sie die Überwurfmutter des Steckers anziehen (Gabelschlüssel SW8). Weitere Informationen dazu finden Sie in den Kapiteln "Anschluss für Industrial Ethernet" und "Anschlüsse für externe Antennen".
   - Spannungsversorgung mit DC 48 V. Verwenden Sie den mit dem SCALANCE W786 gelieferten Stecker. Detailinformationen zur Klemmenbelegung finden Sie im Kapitel "Anschlüsse für die Spannungsversorgung".
   - Spannungsversorgung mit DC 12 - 24 V oder mit AC 110 - 230 V. In diesen Fällen müssen Sie einen Stromversorgungsadapter verwenden (nicht im Lieferumfang des SCALANCE W786 enthalten). Weitere Informationen dazu finden Sie im Kapitel "Anschluss eines Stromversorgungsadapters".
2. Setzen Sie eine Zugentlastungsklammer auf das angeschlossenen Kabel. Der verzahnte Teil der Klammer muss dabei das Kabel vollständig umschließen (wie in Position **B** der vorangegangenen Abbildung dargestellt).

3. Drücken Sie die Zugentlastungsklammer in das Gehäuse, bis die Leitung vollständig an einem Durchbruch der Gehäusedichtung anliegt (Position **C** in der vorangegangenen Abbildung).
4. Verschließen Sie alle Dichtungsdurchbrüche, die Sie nicht für die Zuführung von Leitungen benötigen, mit Blindstopfen (Position **D** in der vorangegangenen Abbildung).
5. Setzen Sie diesen Blindstopfen in eine Zugentlastungsklammer ein. Die untere umlaufende Kerbe muss dabei von der Verzahnung der Zugentlastungsklammer umschlossen werden (wie in der nachfolgenden Abbildung dargestellt). Drücken Sie die Zugentlastungsklammer in das Gehäuse, bis der Blindstopfen vollständig an einem Durchbruch der Gehäusedichtung anliegt.

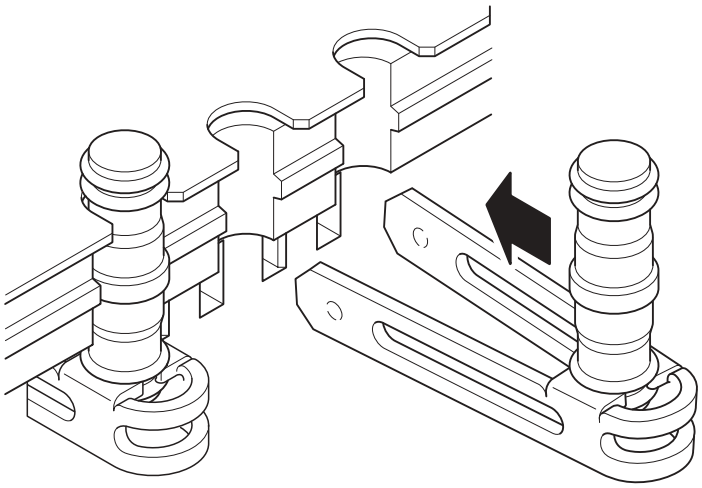


Bild 4-2 Fixierung eines Blindstopfens mit einer Zugentlastungsklammer

Hinweis

Bewahren Sie nicht benutzte Blindstopfen und Zugentlastungsklammern für spätere Verwendung auf.

Besonderheiten beim Anschließen eines ovalen Lichtwellenleiters

Der für die Verwendung mit dem SCALANCE W786 spezifizierte ovale Lichtwellenleiter hat keinen kreisförmigen Querschnitt. Deshalb müssen Sie beim Anschließen dieser Leitungen folgendes berücksichtigen:

Dichtung

Bringen Sie dort, wo der Lichtwellenleiter in der Gehäusedichtung liegt, die mitgelieferte Dichtungsklebefolie an. Nur damit erreichen Sie eine einwandfreie Abdichtung des Gehäuses. Führen Sie dazu folgende Schritte durch:

1. Entfernen Sie die Schutzfolie und wickeln Sie die Dichtungsklebefolie vollständig an der entsprechenden Stelle **quer** um den ovalen Lichtwellenleiter.

Zugentlastungsklammer

Achten Sie beim Aufsetzen der Zugentlastungsklammer auf die richtige Lage des Lichtwellenleiters. Die schmalen Seiten der Leitung müssen Kontakt mit der Verzahnung der Zugentlastungsklammer haben.

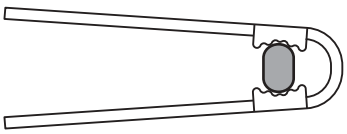


Bild 4-3 Ansicht von oben auf eine Zugentlastungsklammer mit eingelegtem Lichtwellenleiter

4.4 Anschlüsse für die Stromversorgung des SCALANCE W786

Mögliche Versorgungsspannungen

Folgende Versorgungspannungen sind für den SCALANCE W786 geeignet:

- DC 48 V Gleichspannung
  Verwendung des zweipoligen Steckers, der zum Lieferumfang des SCALANCE W786 gehört.
- DC 12 - 24 V Gleichspannung
  Sie verwenden den Stromversorgungsadapter DC 12 - 24 V, der als Zubehör erhältlich ist.
- AC 110 - 230 V Wechselspannung
  Sie verwenden den Stromversorgungsadapter AC 110 - 230 V, der als Zubehör erhältlich ist.
- Power over Ethernet (PoE)
  Wenn ein achtadriges Ethernet-Kabel verwendet wird, dann ist eine Speisung über die vier Adern möglich, die nicht als Datenleitungen verwendet werden. Alternativ kann die Spannung auf die Datenleitungen aufmoduliert werden ("Phantomspeisung").
  Wenn wegen der Feldkonfektionierbarkeit und der höheren mechanischen Robustheit ein Fast-Connect-Ethernet-Stecker benutzt wird, sind nur vieradrige Leitungen verwendbar. In diesem Fall ist nur Phantomspeisung möglich. Eine Einschränkung für den Anwender ergibt sich dadurch nicht, da PoE-kompatible Speiseeinrichtungen immer beide Möglichkeiten vorsehen müssen.

Vorgehensweise beim Anschließen des mitgelieferten Steckers für DC 48 V

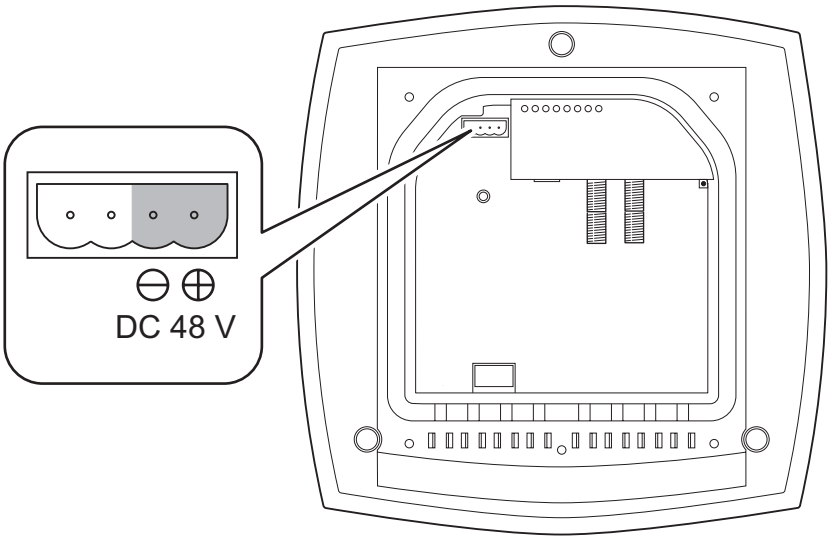


Bild 4-4 Position der Gehäusebuchse für die Stromversorgung bei abgenommenem Gehäusedeckel

Führen Sie folgende Schritte durch, um eine DC 48 V-Leitung an einen SCALANCE W786 anzuschließen:

1. Schließen Sie den mitgelieferten Stecker an die DC 48 V-Leitung an. Die vorangegangene Abbildung zeigt die Lage der Gehäusebuchse und die Kontaktbelegung. Der Stecker ist verpolungssicher und kann nur in die rechte Hälfte der Gehäusebuchse eingesetzt werden. Beachten Sie deshalb beim Anklemmen der Adern, dass der Stecker die in der nachfolgenden Abbildung dargestellte Orientierung hat.

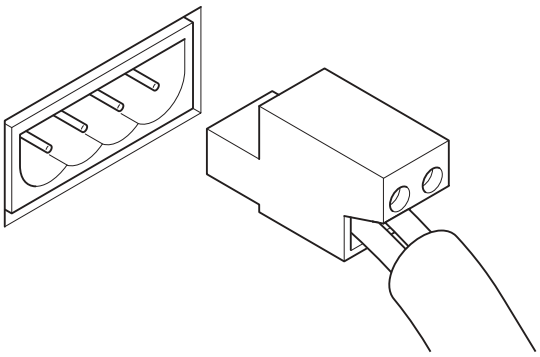


Bild 4-5 Lage des Steckers beim Einsetzen in die Gehäusebuchse

2. Drücken Sie den Stecker in die Gehäusebuchse, bis er dort einrastet.
3. Befestigen Sie die Stromleitung mit einer Zugentlastungsklammer. Entsprechende Informationen finden Sie im Abschnitt "Anschließen der Leitungen".

4.5 Anschließen eines Stromversorgungsadapters

Optionen für die Eingangsspannung

Den optional erhältlichen Stromversorgungsadapter gibt es in zwei Ausführungen:

- Stromversorgungsadapter für DC 12 - 24 V Gleichspannung
- Stromversorgungsadapter für AC 110 - 230 V Wechselspannung

Hinweis

Gilt nur für SCALANCE W786-3xx

Wird ein SCALANCE W786-3xx mit Diversity für drei Antennenpaare betrieben, kann die Stromversorgung für DC 12 - 24 V nicht redundant gespeist werden. In diesem Fall steht für eine zweite Stromleitung kein Durchbruch in der Gehäusedichtung mehr zur Verfügung.

Vorgehensweise beim Einsetzen des Stromversorgungsadapters

⚠ WARNUNG

Lebensgefahr durch Netzspannung

Leitungen für die Stromversorgung dürfen nur in spannungslosem Zustand angeschlossen werden!
Nehmen Sie den SCALANCE W786 erst in Betrieb, nachdem Sie den Gehäusedeckel wieder aufgeschraubt haben und dadurch Schutz gegen die Berührung spannungsführender Teile besteht!

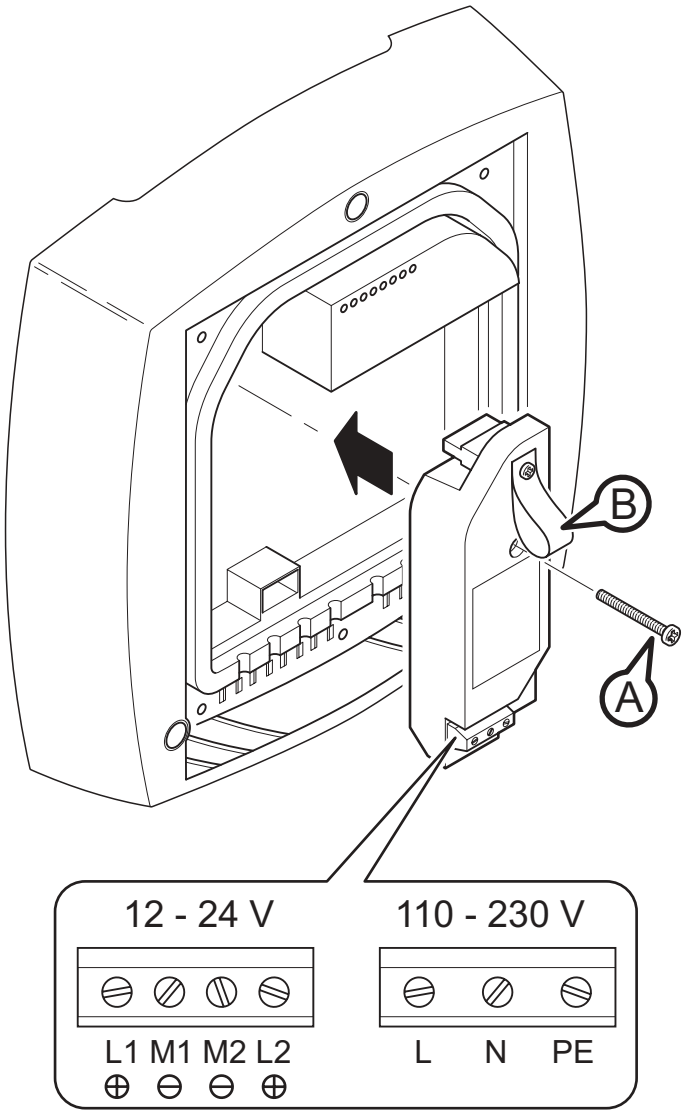


Bild 4-6 Einsetzen eines Stromversorgungsadapters in einen SCALANCE W786

Führen Sie folgende Schritte durch, um einen Stromversorgungsadapter zu montieren und anzuschließen:

1. Setzen Sie den Stromversorgungsadapter, wie in der vorangegangenen Abbildung dargestellt, in den SCALANCE W786 ein. Der Stecker auf der Rückseite des Stromversorgungsadapters muss dabei vollständig in der Gehäusebuchse einrasten. Die Rückseite des Stromversorgungsadapters muss auf der ganzen Fläche an der Innenseite des SCALANCE W786 aufliegen.

VORSICHT
Verwenden Sie ausschließlich die Demontageschlaufe (Position **B** in der vorangegangenen Abbildung), wenn Sie den Stromversorgungsadapter aus dem SCALANCE W786 entnehmen wollen! Dadurch verhindern Sie, dass der Stecker auf der Rückseite des Stromversorgungsadapters verkantet und abbricht.

2. Verbinden Sie den Stromversorgungsadapter und den SCALANCE W786 mit der Schraube, die zum Lieferumfang des Stromversorgungsadapter gehört (Position **A** in der vorangegangenen Abbildung).
3. Schließen Sie die Leitung für die Stromversorgung an. Die Belegung der Klemmen ist in der vorangegangenen Abbildung dargestellt.
4. Befestigen Sie die Leitung für die Stromversorgung mit einer Zugentlastungsklammer. Entsprechende Informationen finden Sie im Abschnitt "Anschließen der Leitungen".

Vorgehensweise beim Entnehmen des Stromversorgungsadapters

Führen Sie folgende Schritte durch, um einen Spannungsversorgungsadapter aus einem SCALANCE W786 zu entnehmen:

⚠ WARNUNG

Lebensgefahr durch Netzspannung

Leitungen für die Stromversorgung dürfen nur in spannungslosem Zustand vom Stromversorgungsadapter getrennt werden!

1. Klemmen Sie die Leitung für die Stromversorgung vom Stromversorgungsadapter ab.
2. Lösen Sie die Befestigungsschraube des Stromversorgungsadapters (Position **A** in der vorangegangenen Abbildung).
3. Ziehen Sie an der Demontageschlaufe(Position **B** in der vorangegangenen Abbildung), um den Stecker auf der Rückseite des Stromversorgungsadapters aus der Gehäusebuchse zu lösen und entnehmen Sie den Stromversorgungsadapter.

4.6 Anschluss für Industrial Ethernet

Gerätevarianten

Beim SCALANCE W786 haben Sie die Wahl zwischen zwei Ethernet-Schnittstellen:

- RJ45-Buchse
- ST-Duplex-Buchse für Multimode-Lichtwellenleiter 1310 nm und einer maximalen Leitungslänge von 3000 m

Vorgehensweise beim Anschließen einer Ethernet-Leitung

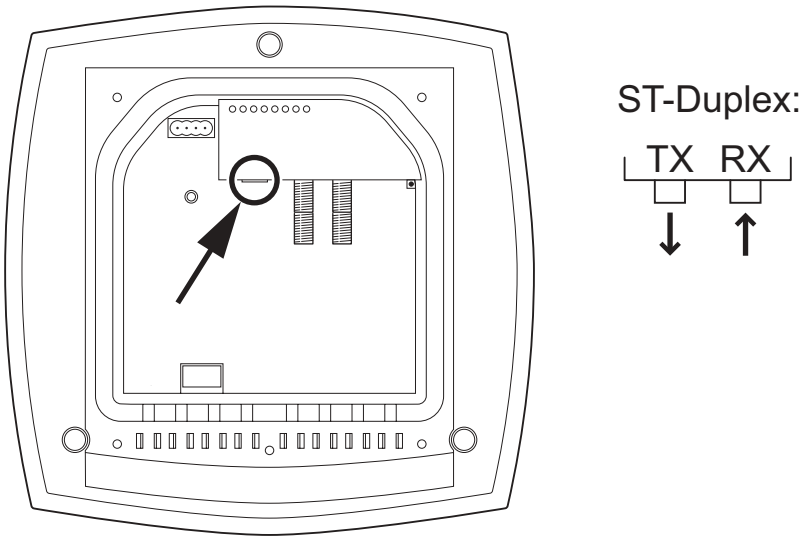


Bild 4-7 Position der Ethernet-Schnittstelle bei abgenommenem Gehäusedeckel

Führen Sie folgende Schritte durch, um eine Ethernet-Leitung an einen SCALANCE W786 anzuschließen:

1. Setzen Sie den Stecker der Ethernet-Leitung in die entprechende Buchse des SCALANCE W786 ein. Achten Sie bei Lichtwellenleitern auf die richtige Zuordnung der sendenden und empfangenden Leitung. Die Lage der Buchse für RX und TX ist in der vorangegangenen Abbildung dargestellt.
2. Befestigen Sie die Ethernet-Leitung mit einer Zugentlastungsklammer. Entsprechende Informationen finden Sie im Abschnitt "Anschließen der Leitungen".

4.7 Anschlüsse für externe Antennen

Vorgehensweise beim Anschließen externer Antennen

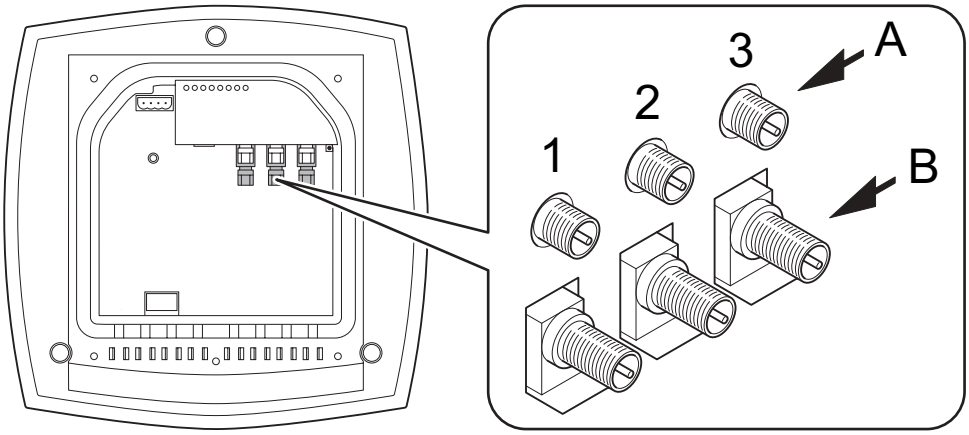


Bild 4-8 Position der Schnittstellen für externe Antennen bei abgenommenem Gehäusedeckel

Für jede WLAN-Schnittstelle gibt es bei einem SCALANCE W786 zwei R-SMA-Buchsen zum Anschluss externer Antennen. Die vorangegangene Abbildung zeigt, wie die R-SMA-Buchsen den WLAN-Schnittstellen zugeordnet sind. Bei einem SCALANCE W786-1PRO ist nur das mit "1" bezeichnete Buchsenpaar vorhanden, bei einem SCALANCE W786-2PRO sind nur die mit "1" und "2" bezeichneten Buchsenpaare vorhanden.

Führen Sie folgende Schritte durch, um eine Leitung für eine externe Antenne an einen SCALANCE W786 anzuschließen:

1. Setzen Sie den Stecker der Antennen-Leitung auf die R-SMA-Buchse und schrauben Sie die Überwurfmutter des Steckers auf die Buchse (Gabelschlüssel SW8), Anzugsmoment 0,6 Nm. Schließen Sie zuerst die Leitung für die Antenne "B" an, wenn Sie für eine Schnittstelle zwei Antennen verwenden wollen.Nach dem Anschließen der Leitung für die Antenne "A" ist die Buchse "B" schlecht zugänglich.
2. Schrauben Sie einen Abschlusswiderstand auf die nicht benutzte Buchse, wenn Sie für eine Schnittstelle nur eine Antenne verwenden.
3. Befestigen Sie die Antennen-Leitung(en) mit einer Zugentlastungsklammer. Entsprechende Informationen finden Sie im Abschnitt "Anschließen der Leitungen".

4.8 Einsetzen / Entnehmen des C-PLUG

Einsetzen des C-PLUG

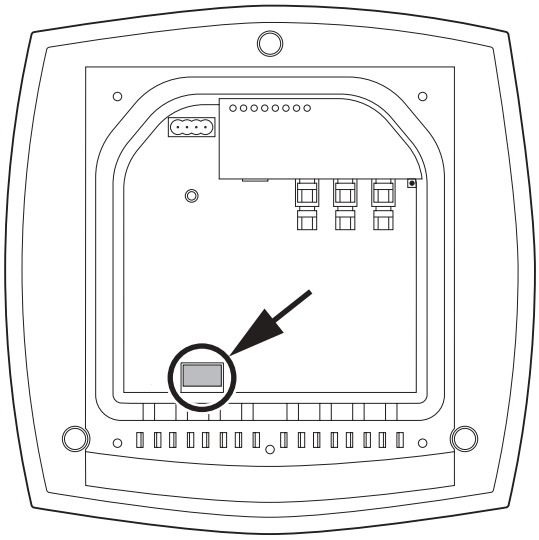


Bild 4-9 Position des Steckplatzes für den C-PLUG bei abgenommenem Gehäusedeckel

Das Gehäuse des C-PLUG hat eine hervorstehende Längskante. Der C-PLUG lässt sich nur einsetzen, wenn sich diese Kante rechts oben befindet. In den Steckplatz des SCALANCE W786 ist an der entsprechenden Stelle eine Fuge eingearbeitet. Sie müssen den C-PLUG vollständig in den Steckplatz einsetzen.

Entnehmen des C-PLUG

Setzen Sie einen Schraubendreher zwischen der rechten Vorderkante des C-PLUG und dem Steckplatz an und lösen Sie den C-PLUG.

Konfigurieren/Projektieren

5

5.1 Technische Grundlagen

5.1.1 Spanning Tree

Vermeidung von Schleifenbildung

Das Spanning Tree-Verfahren ermittelt physikalisch redundante Netzwerkstrukturen und verhindert Schleifenbildung durch Abschalten redundanter Wege. Dazu wertet es die Entfernung, die Leistungsfähigkeit einer Verbindung oder auch Benutzervorgaben aus. Der Datenverkehr erfolgt dann ausschließlich auf den verbleibenden Verbindungswegen.

Wenn der bevorzugte Datenweg ausfällt, sucht der Spanning Tree-Algorithmus den effizientesten Weg, der mit den verbliebenen Netzteilnehmern möglich ist.

Root Bridge und Bridge Priority

Die Ermittlung der effizientesten Verbindung erfolgt immer im Bezug auf die sogenannte "Root Bridge", eine Netzkomponente, die als Wurzelelement einer baumartigen Netzstruktur angesehen wird. Mit dem Parameter "Bridge Priority" können Sie die Wahl der Root Bridge beeinflussen. Der Rechner mit dem geringsten Wert für diesen Parameter wird zwangsläufig Root-Bridge. Wenn zwei Rechner den gleichen Prioritätswert haben, wird derjenige Rechner Root-Bridge, der die niedrigere MAC-Adresse hat.

Verhalten bei Veränderungen der Netztopologie

Wenn Teilnehmer zu einem Netz hinzukommen oder wegfallen hat das möglicherweise Auswirkungen auf die optimale Wegewahl der Datenpakete. Um diese Änderungen zu berücksichtigen, versendet die Root Bridge in regelmäßigen Abständen Konfigurationsmeldungen. Den Zeitabstand zwischen zwei Konfigurationsmeldungen können Sie mit dem Parameter "Hello Time" einstellen.

Aktualität der Konfigurationsinformation

Mit dem Parameter "Max Age" legen Sie das maximale Alter von Konfigurationsinformationen fest. Erhält eine Bridge Konfigurationsinformationen, die älter sind, als in Max Age festgelegt, verwirft Sie diese Meldung und veranlasst eine Neuberechnung der Wege.

Neue Konfigurationsinformationen werden von einer Bridge jedoch nicht sofort, sondern erst nach dem im Parameter "Forward Delay" festgelegten Zeitraum angewendet. So wird sichergestellt, dass der Betrieb entsprechend der neuen Topologie erst gestartet wird, wenn alle Bridges die notwendigen Informationen haben.

5.1.2 iQoS

Clientspezifische Bandbreitenreservierung

iQoS (Quality of Service) ist ein Verfahren, bei dem Clients eine bestimmte Bandbreite zugeordnet bekommen. Aufgrund dieser Zuordnung erfolgt die Datenübertragung zu diesen Clients mit hoher Wahrscheinlichkeit innerhalb eines definierten Zeitraums. Dieses Verfahren kann überall dort sinnvoll eingesetzt werden, wo bestimmte Antwortzeiten gewährleistet werden müssen.

5.1.3 Forced Roaming on IP Down

Funktionsbeschreibung

"Forced Roaming on IP down" überwacht zyklisch die Verbindung zu einer bestimmten IP-Adresse. Hierzu werden ICMP-Pakete verwendet (Echo Request/Reply bzw. Ping). Wenn die IP-Verbindung abbricht, d.h. kein Ping-Reply von der Gegenstelle empfangen wurde, wird an alle WLAN-Clients ein Deauthentication-Frame gesendet. Danach wird das entsprechende WLAN-Interface deaktiviert.

Die IP-Verbindung wird nun weiterhin überwacht und das WLAN-Interface wieder aktiviert, sobald der Access Point ein Ping-Reply von der Gegenstelle empfängt.

Mit diesem Mechanismus ist es z. B. möglich, eine Verbindung zwischen wireless Clients und einem Server zu überwachen. Ist der Server über den Access Point nicht mehr erreichbar, werden die Clients deauthentifiziert und das WLAN-Interface des Access Points abgeschaltet. Die Clients roamen und verbinden sich dann auf einen anderen Access Point, von dem aus der Server erreichbar ist. Sobald der erste Access Point den Server wieder erreicht, schaltet er seine WLAN-Interfaces wieder aktiv.

5.1.4 Link Check

Gerätebezogene Verbindungsüberwachung

Die Funktion Link Check bietet eine gerätebezogenen Verbindungsüberwachung für maximal zehn drahtlose Teilnehmer, die am SCALANCE W78x angemeldet sind. Zu vergleichen ist dieser Dienst mit dem Link an einer drahtgebundenen Verbindung. Überwacht wird, ob der Teilnehmer über das drahtlose Medium erreichbar ist. Wird nach der Hälfte der konfigurierten Überwachungszeit kein Paket vom Teilnehmer empfangen oder erfolgreich gesendet, versucht der SCALANCE W78x dem Teilnehmer ein Testpaket zu senden.

5.1.5 Redundanz

Redundante Verbindung zwischen zwei SCALANCE W78x

Zwei SCALANCE W78x mit mehr als einer Funkschnittstellen können Sie so konfigurieren, dass eine redundante Funkverbindung entsteht. Die Redundanzfunktion bewirkt dabei das automatische Umschalten auf die zweite Funkschnittstelle, wenn über die erste Funkschnittstelle kein Datentransfer möglich ist.Der Anwender wird über den Zustand der redundanten Verbindung mit den Zuständen "not connected" (nicht verbunden), "connected" (verbunden) oder "error" (Kommunikationsfehler) informiert.

5.1.6 IP-Alive

Anwendungsbezogene Verbindungsüberwachung

Die Funktion IP-Alive bietet eine anwendungsbezogene Verbindungsüberwachung der Funkstrecke.

IP-Alive kann sinnvoll auf IP-Verbindungen angewendet werden, von denen bekannt ist, dass über sie zyklisch Daten versendet werden. Bei IP-Alive legen Sie eine Überwachungszeit für eine IP-Adresse und einen Port fest. Falls Sie keinen bestimmten Port sondern nur den Datenverkehr von einer bestimmten IP-Adresse überwachen wollen, dann tragen Sie beim Port einfach eine 0 ein. Damit wird die Überwachung bei jedem Telegramm von dieser IP-Adresse zurückgesetzt.

Im Gegensatz zu Link Check findet bis zum Ablauf der Überwachungszeit keine Überprüfung durch den SCALANCE W78x statt. Der SCALANCE W78x prüft passiv, ob im vorgegebenen Überwachungszeitraum Kommunikation stattgefunden hat. Wie auch beim Link Check können hier bis zu zehn Verbindungen eingetragen werden.

5.1.7 MAC-basierte Kommunikation

Auto Find Adopt MAC / Adopt MAC manually

Telegramme in Richtung vom Client zum Access Point enthalten als Source-MACAdresse immer die MAC-Adresse des WLAN-Interfaces. Somit ist in der LearningTable auf der Access Point-Seite immer nur die MAC-Adresse des WLAN-Interfaces des Clients zu finden. Wird die MAC-Adresse eines Geräts adoptiert, das am Client angeschlossen ist, erreichen sowohl die MAC-basierten als auch die IP-basierten Telegramme für genau dieses Gerät ihr Ziel.

Weitere Teilnehmer, die sich hinter dem Client befinden, können nicht angesprochen werden. Der Access Point prüft, ob die Ziel-MAC-Adresse mit den MAC-Adressen der verbundenen Clients übereinstimmt. Da ein Client nur eine MAC-Adresse adoptieren kann, findet der Access Point keine Übereinstimmung und verwirft die Pakete mehrerer Teilnehmer.

Maximal mögliche Anzahl MAC-Teilnehmer hinter dem Client: 1

Hinweise zur Einstellung "Auto Find Adopt MAC":

- Solange an der Ethernet-Schnittstelle kein Link besteht, nutzt das Gerät die MAC-Adresse der Ethernet-Schnittstelle, um in diesem Zustand ansprechbar zu sein. In diesem Zustand kann das Gerät über das Primary Setup Tool gefunden werden.
- Sobald an der Ethernet-Schnittstelle ein Link besteht, adoptiert das Gerät die Quell-MAC-Adresse des ersten empfangenen Telegramms.

Hinweis

Ab dem Zeitpunkt, an dem das Gerät eine fremde MAC-Adresse adoptiert hat (sei es manuell oder automatisch), antwortet das Gerät nicht mehr auf Anfragen des Primary Setup Tools, wenn die Anfrage über die WLAN-Schnittstelle empfangen wird. Anfragen des PST über die Ethernet-Schnittstelle werden weiterhin beantwortet.

Adopt Own MAC (nur für W746-1 und W747-1 bzw. W746-1PRO und W747-1RR sowie W78x im Client Modus)

Sollen IP-basierte Telegramme an ein hinter dem Client angeschlossenen Gerät gesendet werden, kann die Defaulteinstellung Adopt Own Mac beibehalten werden. Der Client meldet sich mit der MAC-Adresse seiner Ethernet-Karte an. Die IP-Pakete werden über eine intern gehaltene Tabelle aufgeschlüsselt und an die angeschlossenen Geräte weitergeleitet (IP-Mapping).

Eine Kommunikation auf MAC-Adressen-Ebene (ISO/OSI Schicht Zwei) kann nur dann zu einer Komponente hinter dem Client erfolgen, wenn deren MAC-Adresse vom Client adoptiert wurde.

Maximal mögliche Anzahl MAC-Teilnehmer hinter dem Client: 1

Layer-2-Tunneling (nur für W746-1 und W747-1 bzw. W746-1PRO und W747-1RR sowie W78x im Client Modus)

Beim Layer-2-Tunneling liefert der Client beim Anmelden an einem Access Point Informationen über die hinter ihm angeschlossenen Geräte mit. Damit ist der Eintrag der MAC-Adressen dieser Geräte in die Learning Table des Access Points möglich. Der Access Point kann MAC-basierte Telegramme zu den Geräten hinter dem Client an den entsprechenden Client weiterleiten.

Dabei wird ähnlich wie bei WDS ein eigener Port für den L2T-Client angelegt, durch den die Ethernet-Telegramme ohne Änderung der Ziel-MAC-Adreesse versendet werden.

Maximal mögliche Anzahl MAC-Teilnehmer hinter dem Client: 8

5.1.8 IP-basierte Kommunikation

IP-Mapping (nur für W746-1 und W747-1 bzw. W746-1PRO und W747-1RR sowie W78x im Client Modus)

Sind hinter dem Client mehrere Geräte angeschlossenen, die nur mit IP-Telegrammen angesprochen werden sollen, können Sie mit einem Client mehreren Geräten den WLAN-Zugang ermöglichen. Bei dem sogenannten IP-Mapping unterhält der Client eine Tabelle mit der Zuordnung von MAC-Adresse und IP-Adresse, um eingehende IP-Telegramme an die richtige MAC-Adresse zu verschicken.

Maximal mögliche Anzahl IP-Teilnehmer hinter dem Client: 8

5.2 Vergabe einer IP-Adresse

5.2.1 Aufbau einer IP-Adresse

Adressklassen nach RFC 1518 und RFC 1519

IP-Adressbereich	Max. Anzahl der Netzwerke	Max. Anzahl Hosts/Netzwerk	Klasse	CIDR
1.x.x.x bis 126.x.x.x	126	16777214	A	/8
128.0.x.x bis 191.255.x.x	16383	65534	B	/16
192.0.0.x bis 223.255.255.x	2097151	254	C	/24
Multicast-Gruppen			D	
Reserviert für Experimente			E	

Eine IP-Adresse besteht aus 4 Bytes. Jedes Byte wird dezimal dargestellt und ist durch einen Punkt vom vorherigen getrennt. Es ergibt sich also folgender Aufbau, wobei für XXX eine Zahl zwischen 0 und 255 zu setzen ist:

XXX.XXX.XXX.XXX

Die IP-Adresse besteht aus zwei Teilen, der Netzwerkadresse und der Endteilnehmeradresse. Dadurch ist es möglich, verschiedene Teilnetze zu bilden. Abhängig davon, welche Bytes der IP-Adresse als Netzwerkadresse und welche als Endteilnehmeradresse genutzt werden, kann eine IP-Adresse einer bestimmten Adressklasse zugeordnet werden:

Subnetz-Maske

Die Bits der Endteilnehmer-Adresse können für die Bildung von Subnetzen verwendet werden. Dabei stellen die führenden Bits die Adresse des Subnetzwerks dar, die restlichen Bits werden als Adresse des Rechners im Subnetz interpretiert.

Ein Subnetz wird durch die Subnetzmaske definiert. Der Aufbau der Subnetzmaske entspricht dem einer IP-Adresse. Ist in der Subnetzmaske an einer Bitposition eine "1" gesetzt, gehört das Bit an der entsprechenden Stelle in der IP-Adresse zur Subnetzadresse, andernfalls zur Adresse des Rechners.

Beispiel für ein Klasse B-Netz:

Die Standard-Subnetz-Adresse für Klasse B-Netze ist 255.255.0.0, es stehen also die letzten beiden Bytes für die Festlegung eines Subnetzes zur Verfügung. Wenn 16 Teilnetze definiert werden sollen, muss das dritte Byte der Subnetzadresse auf 11110000 (Binärdarstellung) gesetzt werden. In diesem Fall ergibt sich die Subnetzmaske 255.255.240.0.

Um festzustellen, ob zwei IP-Adressen zum gleichen Subnetz gehören, werden auf die beiden IP-Adressen und die Subnetzmaske eine bitweise UND-Verknüpfung angewendet. Wenn beide Verknüpfungen das gleiche Ergebnis haben, gehören beide IP-Adressen zum gleichen Subnetz, wie z. B. 141.120.246.210 und 141.120.252.108.

Außerhalb des lokalen Netzwerks ist die beschriebene Aufteilung der Endteilnehmer-Adresse ohne Bedeutung, dort ist für die Paketvermittlung nur die IP-Adresse in ihrer Gesamtheit von Interesse.

Hinweis

In der Bit-Darstellung der Subnetz-Maske müssen die "Einsen" linksbündig gesetzt sein (es dürfen keine "Nullen" zwischen den "Einsen" stehen).

5.2.2 Erstmalige Vergabe einer IP-Adresse

Konfigurationsmöglichkeiten

Die erstmalige Vergabe einer IP-Adresse für einen SCALANCE W-700 kann nicht mit dem Web Based Management oder dem Command Line Interface über TELNET erfolgen, weil diese Konfigurations-Werkzeuge bereits eine IP-Adresse voraussetzen.

Es gibt folgende Möglichkeiten, einem unkonfigurierten Gerät ohne IP-Adresse eine solche Adresse zuzuweisen:

- DHCP (Default)
- STEP 7
- NCM PC
- Primary Setup Tool

Hinweis

DHCP ist im Auslieferungszustand und nach "Restore Factory Defaults and Restart" eingeschaltet. Wenn ein DHCP-Server im lokalen Netz verfügbar ist und dieser auf den DHCP-Request eines SCALANCE W-700 antwortet, so werden schon beim ersten Hochlauf automatisch IP-Adresse, Subnetzmaske und Gateway zugeteilt. Durch "Reset to Memory Defaults" wird weder eine durch DHCP noch eine vom Benutzer vergebene IP-Adresse gelöscht.

5.2.3 Adressvergabe über DHCP

Eigenschaften von DHCP

DHCP (Dynamic Host Configuration Protocol) ist ein Verfahren zur automatischen Vergabe von IP-Adressen. Es hat folgende Eigenschaften:

- DHCP kann sowohl während des Hochlauf eines Geräts als auch im laufenden Betrieb eingesetzt werden.
- Die vergebene IP-Adresse bleibt nur für einen bestimmten Zeitraum, die sogenannte Lease Time, gültig. Nach Ablauf dieser Zeitdauer muss der Client entweder eine neue IP-Adresse anfordern oder die Gültigkeitsdauer der vorhandenen IP-Adresse verlängern.
- Es erfolgt normalerweise keine feste Adresszuordnung, d. h. wenn ein Client erneut eine IP-Adresse anfordert, erhält er in der Regel eine andere Adresse als bei der vorhergehenden Anforderung. Es gibt aber die Möglichkeit, den DHCP-Server so zu konfigurieren, dass er eine feste Adresszuordnung vornimmt.

Hinweis

DHCP sieht einen Mechanismus vor, nach dem die IP-Adresse nur für eine begrenzte Zeitdauer (Lease Time) zugeteilt wird. Wenn nach Ablauf der LeaseTime das Gerät den DHCP Server nicht für einen erneuten Request erreicht, werden die zugewiesene IP-Adresse, die Subnetz-Maske und das Gateway in statische Einträge überführt.

Das Gerät ist folglich auch ohne DHCP Server weiterhin unter der zuletzt vergebenen IP Adresse erreichbar. Dies entspricht nicht dem Standard-Verhalten von Office Geräten, ist jedoch für einen reibungslosen Anlagenbetrieb notwendig.

Da der DHCP-Client aber zusätzlich ein RELEASE an den Server absetzt, kann der Server diese Adresse an ein weiteres Gerät vergeben, wodurch es zu Inkonsistenzen im Netz kommen kann.

Abhilfe:

Nach dem Abschalten von DHCP sollten Sie deshalb

- die IP-Adresse des Geräts auf eine nicht von DHCP vergebene Adresse ändern

oder

- die dem Gerät zugeordnete IP-Adresse aus dem Adressband des DHCP-Servers entfernen.

Ein Mischbetrieb von dynamischer Adressvergabe und statisch vergebenen Adressen ist grundsätzlich nicht empfehlenswert.

5.2.4 Adressvergabe mit dem Primary Setup Tool

Einleitung

Das PST (Primary Setup Tool) ist in der Lage, unkonfigurierten Geräten ohne IP-Adresse eine solche Adresse zuzuweisen.

Voraussetzung

Voraussetzung ist, dass die Geräte über eine voreingestellte Ethernet (MAC)- Adresse verfügen und im Netz online erreichbar sind.

Hinweis

Weitere Informationen zur Benutzung finden Sie im Projektierungshandbuch Primary Setup Tool.

Sie finden das PST bei Siemens Automation and Drives Service & Support im Internet unter der Beitrags-ID 19440762. Diesen Beitrag erreichen Sie unter folgender URL:

http://support.automation.siemens.com/WW/view/de/19440762

5.3 Die Wizards des Web Based Management

5.3.1 Einleitung

Prinzip des Web Based Managements

Der SCALANCE W-700 verfügt über einen integrierten HTTP-Server für das Web Based Management. Wird der SCALANCE W-700 über einen Internet-Browser angesprochen, liefert er abhängig von den Benutzereingaben HTML-Seiten an den Client-Rechner zurück.

Der Benutzer trägt seine Konfigurationsdaten in die vom SCALANCE W-700 gesendeten HTML-Seiten ein. Der SCALANCE W-700 wertet diese Informationen aus und erzeugt dynamisch Antwortseiten.

Der besondere Vorteil dieses Funktionsprinzips ist, dass auf der Clientseite außer einem Internet-Browser keine besondere Software erforderlich ist.

Voraussetzungen für Web Based Management

Nachdem Sie dem Gerät mit dem Primary Setup Tool eine IP-Adresse zugewiesen haben, können Sie die weitere Konfiguration mit dem Web Based Management durchführen.

Um das Web Based Management nutzen zu können, ist eine kabelgebundene Netzverbindung zwischen dem SCALANCE W-700 und dem Clientcomputer zweckmäßig. Prinzipiell ist die Nutzung des Web Based Managements auch über ein Funknetz möglich, allerdings kann der SCALANCE W-700 so eingestellt werden, dass der Zugriff über das Funknetz deaktiviert ist.

Es wird empfohlen, Microsoft Internet Explorer ab Version 5.5 oder Mozilla Firefox ab Version 1.5 zu verwenden.

Alle Seiten des Web Based Managements erfordern JavaScript. Achten Sie deshalb auf eine entsprechende Browsereinstellung.

Da das Web Based Management HTTP-basiert ist, müssen Sie bei installierter Firewall den Zugriff auf Port 80 bzw. Port 443 für HTTPS ermöglichen.

Hinweis

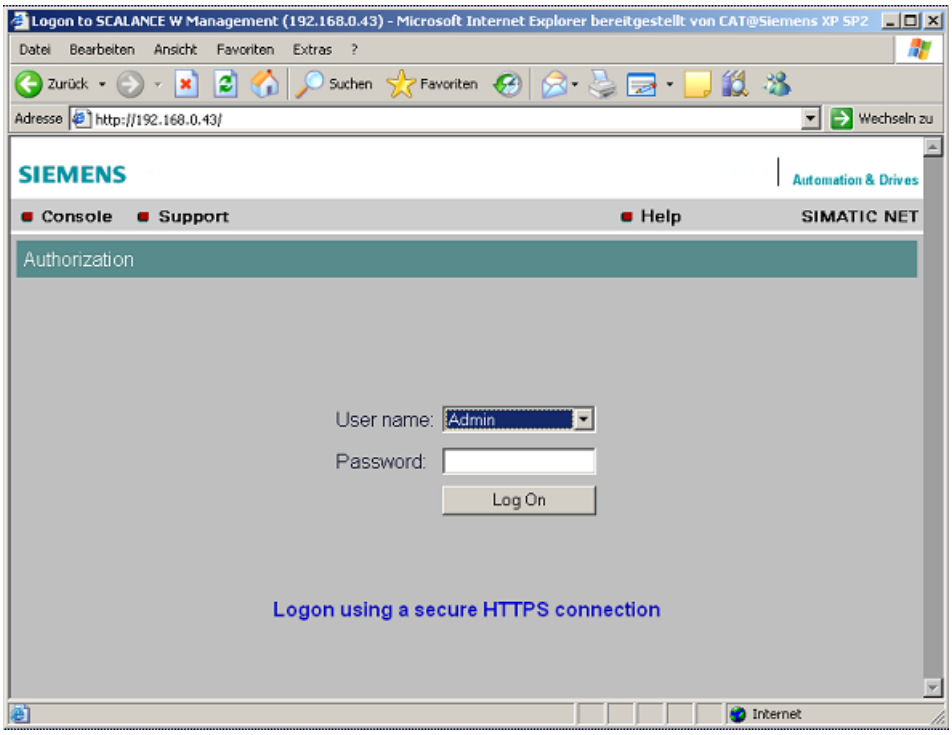
Die in diesem Kapitel dargestellten Screenshots wurden unter Verwendung des Microsoft Internet Explorers Version 6.0 erstellt. Bei Verwendung anderer Browser (z.B. Mozilla) kann das Erscheinungsbild der Menüs abweichen.

5.3.2 Starten des Web Based Managements und Anmeldung

Vorgehen

Führen Sie folgende Schritte durch, um mit einem Internet Browser eine Verbindung zu einem Gerät herzustellen:

1. Geben Sie im Adressfeld des Internet-Browsers die IP-Adresse oder die URL des SCALANCE W-700 ein. Wenn eine einwandfreie Verbindung zum SCALANCE W-700 besteht, erscheint die Login-Maske des Web Based Managements:



2. Wählen Sie in der Klappliste "User name" den Eintrag "Admin", wenn Sie Einstellungen des SCALANCE W-700 verändern wollen (lesender und schreibender Zugriff). Wenn Sie den Eintrag "User" wählen, haben Sie nur lesenden Zugriff auf die Konfigurationsdaten des SCALANCE W-700.
3. Geben Sie Ihr Passwort ein. Falls Sie noch kein Passwort festgelegt haben, gelten die Default-Passwörter des Auslieferungszustands: Geben Sie admin ein, wenn Sie als User name "Admin" ausgewählt haben oder user, wenn Sie "User" ausgewählt haben.
4. Klicken Sie die Schaltfläche "Log On", um die Anmeldung zu starten.

Hinweis

Für die US-Variante des SCALANCE W-700 ist das Passwort für den Benutzer "admin" geändert, kann aber durch Fachpersonal für professionelle WLAN Installationen beim Siemens Support erfragt werden.

Verbindung über HTTPS

Das Web Based Management bietet auch die Möglichkeit, sich über die gesicherte Verbindung des HTTPS-Protokolls mit dem Gerät zu verbinden.

Nutzen Sie den Link "Logon using a secure HTTPS connection" in der Anmeldemaske (siehe vorangegangene Abbildung) oder geben Sie im Adressfeld des Internet-Browsers "https://" und die IP-Adresse des SCALANCE W7xx ein und bestätigen Sie mit Enter. Es erscheint die Warnmeldung "Security Alert", in der Sie gefragt werden, ob Sie den Vorgang fortsetzen möchten. Bestätigen Sie mit "YES". Die Login-Maske des Web Based Managements erscheint.

5.3.3 Auswahl der Wizards

Basic Wizard, Security Wizard und iPCF-Wizard

Das Web Based Management bietet mehrere Wizards an, die eine problemlose Inbetriebnahme ohne Detailkenntnisse der Wireless-Technologie ermöglichen. Ein Wizard besteht aus einer Abfolge von Bildschirm-Masken, in die Sie grundlegende Konfigurationsdaten eintragen.

Es gibt folgende Wizards:

- **Basic Wizard**
  Für allgemeine Einstellungen, damit die Basisfunktionalität des Geräts gewährleistet ist.
- **Security Wizard**
  Der Wizard für die Sicherheitseinstellungen unterstützt Sie bei der Festlegung sicherheitsrelevanter Parameter.
- **iPCF-Wizard**
  Dieser Wizard steht für die Konfiguration des iPCF-Verfahrens (**i**ndustrial **P**oint **C**oordination **F**unction) zur Verfügung.

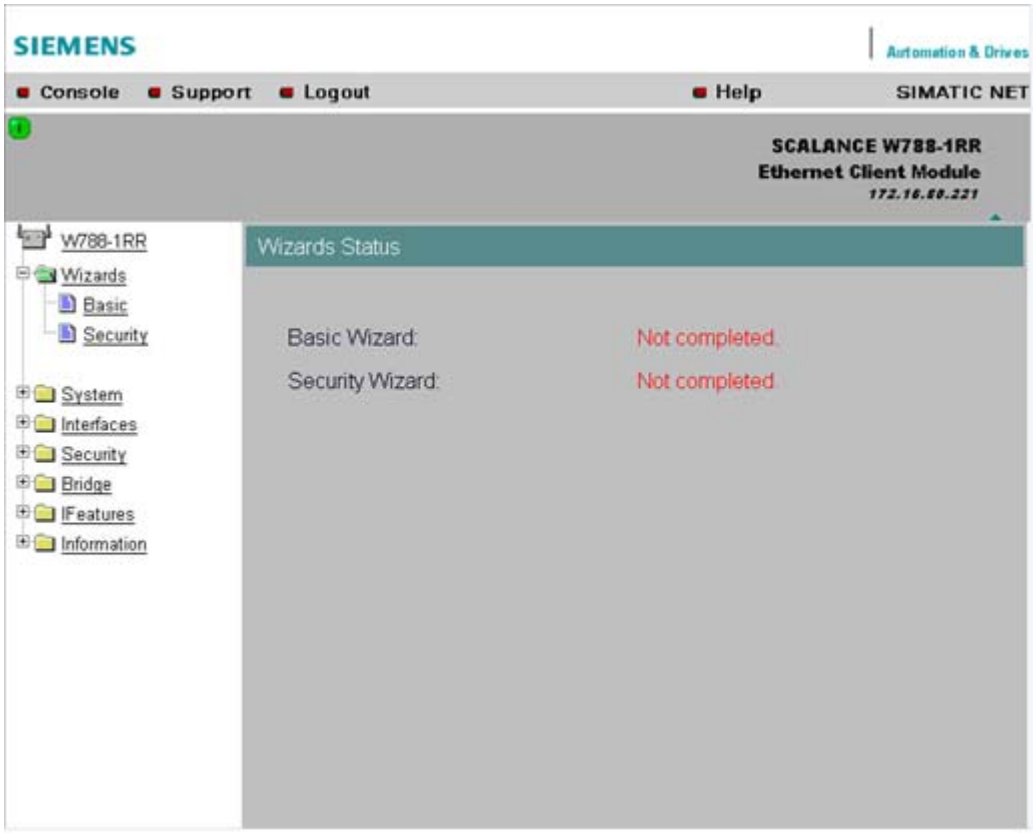
Hinweis

Der iPCF-Wizard ist nur für folgende Geräte verfügbar:

- SCALANCE W78x-xRR
- SCALANCE W747-1
- SCALANCE W747-1RR

Wizard Status

Nach der Auswahl des Menüs "Wizards" im linken Teil der Bildschirm-Maske wird für alle Wizards der Bearbeitungszustand angezeigt. Wenn Sie einen Wizard bearbeitet haben, wird als Status "Done" angezeigt. Wenn Sie alle Wizards bearbeitet haben, wird außerdem der Eintrag "Wizards" in der Menüauswahl an das untere Ende gesetzt.



Hinweis

Einige Seiten der Wizards haben im Access Point-Modus und in der Betriebsart "Client" unterschiedlichen Inhalt. In diesen Fällen gibt es für beide Alternativen eine eigene Beschreibung.

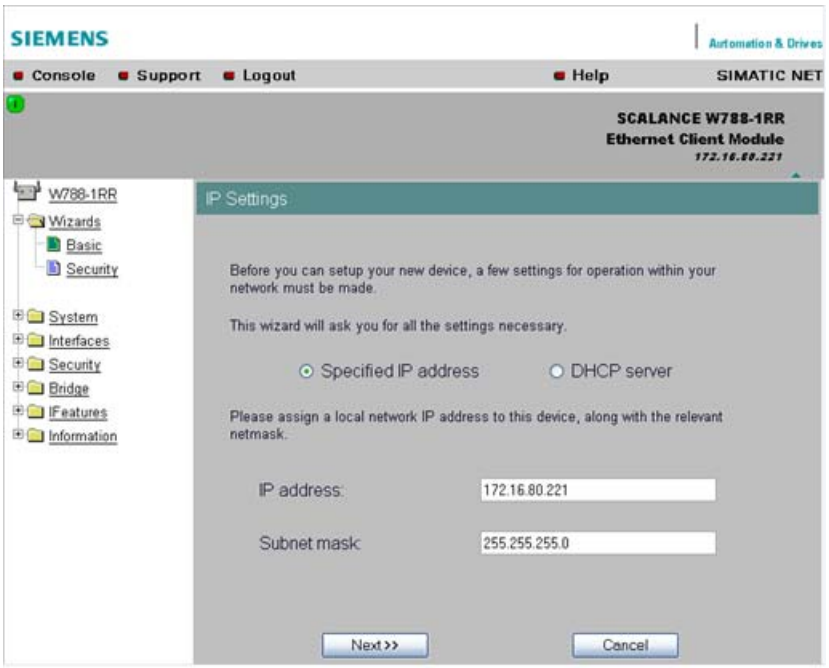
Die Betriebsart können Sie im Menü "System" festlegen.

5.4 Basic Wizard

5.4.1 IP-Einstellungen

Beschreibung

Zu den grundlegenden Konfigurationsschritten für ein Ethernet-Gerät gehört die Festlegung der IP-Adresse. Mit der IP-Adresse wird ein Gerät im Netz eindeutig identifiziert. Auf dieser Seite machen Sie Angaben zur IP-Konfiguration des SCALANCE W-700.



Optionsfelder *Specified IP address / DHCP server*

Für die Zuordnung von IP-Adressen zu Geräten gibt es zwei Möglichkeiten: Die Vergabe einer unveränderlichen Adresse für ein Gerät und der Bezug einer dynamischen IP-Adresse von einem DHCP-Server. Wählen Sie "Specified IP Address", wenn Sie keinen DHCP-Server verwenden.

Eingabefeld *IP address*

Die IP-Adresse des SCALANCE W-700. Geben Sie hier eine Adresse ein, die innerhalb Ihres Netzes eindeutig ist.

Eingabefeld *Subnet mask*

Die Subnetz-Maske legt fest, in welchem Adressband Kommunikation stattfinden kann.

Die vier durch Punkte getrennten Zahlen einer IP-Adresse werden dabei als Bitmuster interpretiert. Ist an einer Bitposition der Subnetzmaske eine Eins gesetzt, hat das zur Folge, dass nur Geräte mit einer solchen IP-Adresse mit dem SCALANCE W-700 Management Agent kommunizieren können, die an dieser Bitposition mit der IP-Adresse des SCALANCE W-700 übereinstimmt.

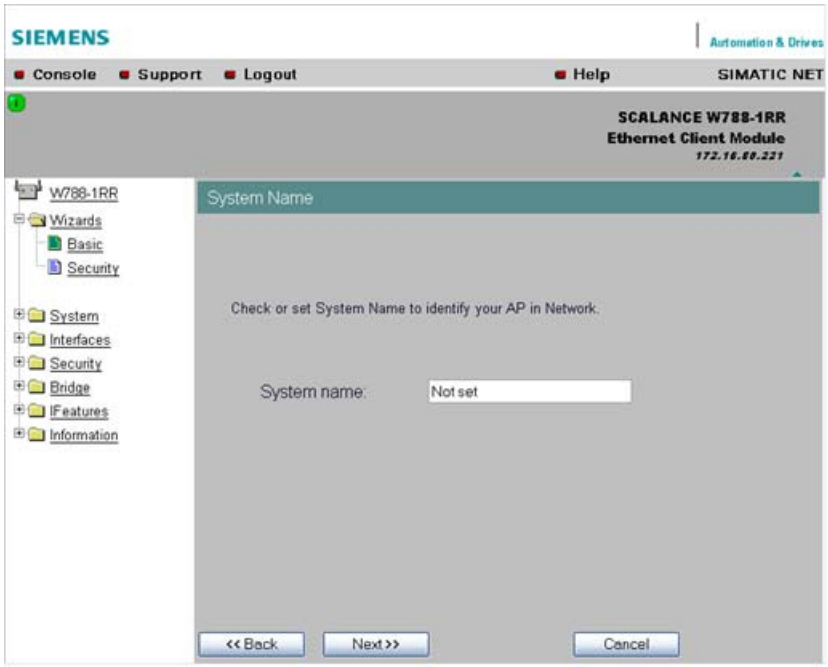
Beispiel

Die IP-Adresse des SCALANCE W-700 sei 192.168.147.189, die Subnetzmaske 255.255.255.0. Das Bitmuster für 255 ist 1111 1111. Daraus folgt, dass das Bitmuster der ersten Zahl der IP-Adresse eines Kommunikationspartners genau dem Bitmuster der IP-Adresse des SCALANCE W-700 an dieser Stelle entsprechen muss. Gleiches gilt für den zweiten und dritten Teil der IP-Adresse. Die IP-Adresse eines Kommunikationspartners muss also mit 192.168.147 beginnen. Das Bitmuster von 0 ist 0000 0000. Deshalb braucht das Bitmuster des letzten Teils der IP-Adresse des Partnergeräts an keiner Stelle der Adresse des SCALANCE W-700 zu entsprechen, kann also beliebig sein.

5.4.2 System Name

Beschreibung

Der Systemname identifiziert einen Netzteilnehmer, ist aber für den Anwender aussagekräftiger als die IP-Adresse.



Eingabefeld *System name*

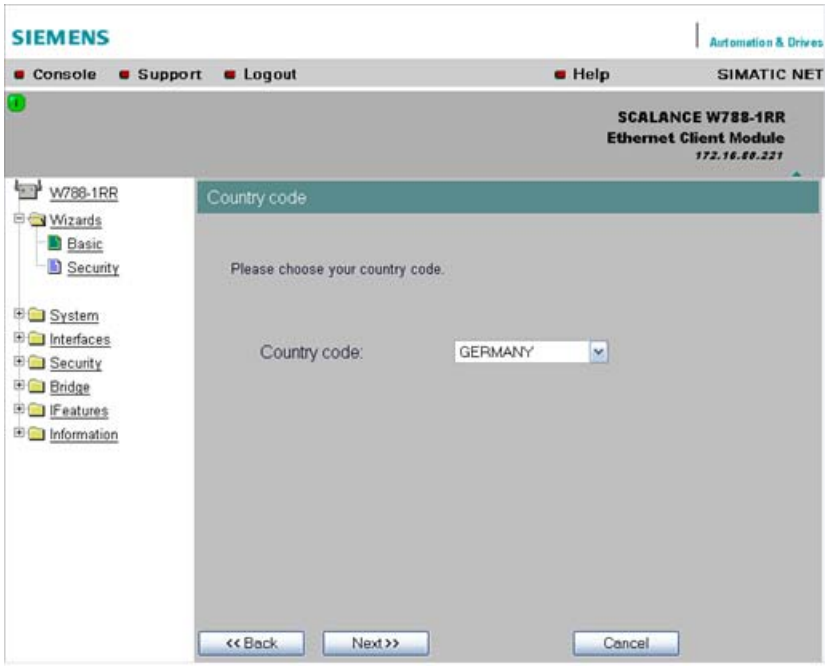
Tragen Sie in dieses Feld den Systemnamen für ihren SCALANCE W-700 ein. Dieser Parameter entspricht dem SNMP-Parameter "sysName". Der Systemname darf maximal 255 Zeichen lang sein. Wenn Sie diesen Parameter auch für WDS oder Redundanz nutzen wollen, beträgt die maximale Länge 30 Zeichen.

5.4.3 Country Code

ACHTUNG
Die richtige Ländereinstellung ist für einen zulassungskonformen Betrieb unbedingt notwendig. Die Auswahl eines vom Anwenderland abweichenden Landes kann strafrechtlich geahndet werden!

Beschreibung

Für die drahtlose WLAN-Kommunikation gelten in verschiedenen Ländern teilweise unterschiedliche Einteilungen der Frequenzbänder in Kanäle. Zusätzlich unterscheiden sich die länderspezifischen Bestimmungen auch in der Festlegung der maximalen Sendeleistung. Bei der Konfiguration des SCALANCE W-700 müssen Sie festlegen, welche lokalen Nutzungsbestimmungen für Sie relevant sind. Dies legen Sie über den Parameter "Country Code" fest.



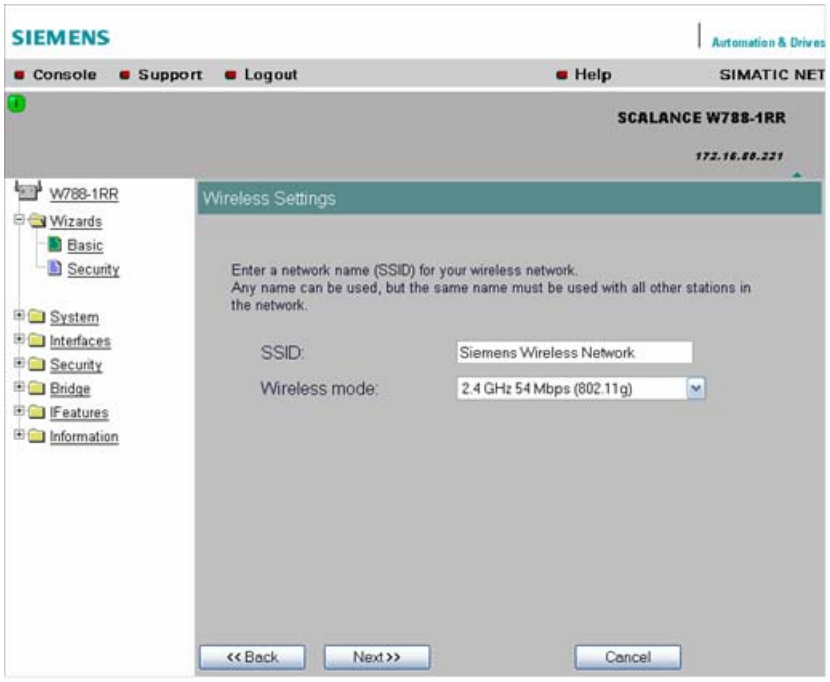
Klappliste *Country code*

Wählen Sie aus dieser Liste das Land aus, in dem der SCALANCE W-700 betrieben wird. Sie brauchen die landesspezifischen Daten nicht zu kennen, die richtige Kanaleinteilung und Festlegung der Sendeleistung erfolgt entsprechend Ihrer Länderauswahl durch den SCALANCE W-700.

5.4.4 Wireless-Einstellungen im Access Point-Modus

Beschreibung

Auf dieser Seite legen Sie die Konfiguration des drahtlosen Netzwerkes fest. Dazu gehören der Netzwerkname und das Übertragungsverfahren. Wenn Sie einen SCALANCE W78x mit mehreren WLAN-Schnittstellen konfigurieren, erscheint diese Seite für jede WLAN-Schnittstelle. Sie können für die einzelnen WLAN-Schnittstellen unterschiedliche Einstellungen vornehmen.



Eingabefeld *SSID*

Tragen Sie in dieses Feld den Namen Ihres Netzwerks ein. Der SCALANCE W78x ermöglicht es, für die SSID alle Zeichen außer dem Prozentzeichen zu verwenden. Aus Gründen der Kompatibilität zu Partnergeräten sollten Sie allerdings keine sprachspezifischen Buchstaben (zum Beispiel deutschen Umlaute) oder Sonderzeichen verwenden. Die Zeichenkette für SSID darf maximal 32 Zeichen lang sein.

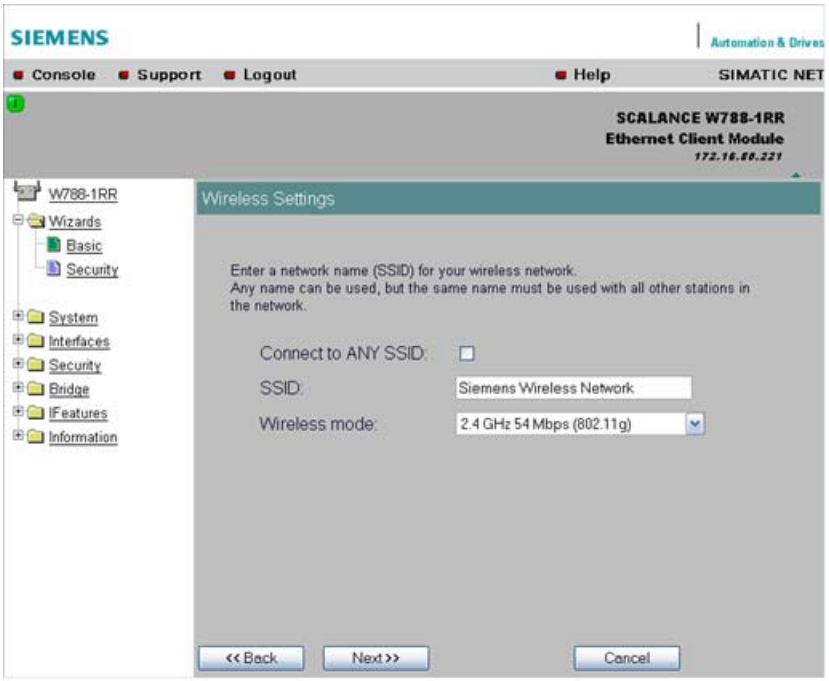
Klappliste *Wireless Mode*

Wählen Sie ein Übertragungsverfahren aus, das von allen Partnergeräten unterstützt wird. Bei einem SCALANCE W78x mit mehreren WLAN-Schnittstellen kann es zweckmäßig sein, für jede WLAN-Schnittstellen ein anderes Übertragungsverfahren einzustellen, um unterschiedliche Clients optimal zu unterstützen. Die Einstellung "802.11.b" bzw "802.11.g" bewirkt, dass alle Einstellungen im Menü "Advanced G"nach Möglichkeit berücksichtigt werden, aber Kompatibilität zu Geräten gegeben ist, die konform zu IEEE 802.11b sind.

5.4.5 Wireless-Einstellungen im Client-Modus

Beschreibung

In der Betriebsart "Client" gibt es zusätzlich noch das Optionskästchen "Connect to ANY SSID". Die sonstigen Einstellungen entsprechen denen des Access Point-Modus.



Optionskästchen *Connect to ANY SSID*

Wenn dieses Optionskästchen markiert ist, verbindet sich der Client mit dem Access Point, der einen bestmöglichen Datentransfer ermöglicht und zu dem eine Verbindung aufgrund der Sicherheitseinstellungen erlaubt ist.

5.4.6 Adopt MAC Address Einstellungen (Nur für Clients oder Access Points im Client-Modus)

Zuordnung der MAC-Adresse

Für das an der Ethernet-Schnittstelle des SCALANCE W-700-Clients angeschlossene Gerät muss zur Erreichbarkeit eine MAC-Adresse festgelegt werden. Diese MAC-Adresse wird vom Client zur Funkkommunikation mit dem Access Point verwendet.

Es gibt mehrere Möglichkeiten, wie dies erfolgen kann:

- Wenn hinter dem Client genau eine MAC-Adresse bedient werden soll, gibt es zwei Möglichkeiten, wie dies erfolgen kann:
  - Automatisch
    Der Client nimmt die Source-MAC-Adresse des ersten Telegramms, welches er über die Ethernet-Schnittstelle empfängt.
  - Manueller Eintrag durch den Benutzer.
- Wenn hinter dem Client bis zu acht MAC-Adressen bedient werden sollen, steht das "Layer 2 Tunneling" zur Verfügung:

Diese Einstellung erfüllt Forderungen von Industrie-Applikationen, bei denen MAC-Adressen-basierte Kommunikation an mehrere Geräte hinter dem Client benötigt wird. Clients mit dieser Einstellung können sich nicht auf Standard-Wifi-Geräte und SCALANCE W700-Access Points mit Firmware V3.0 oder älter verbinden.

Hinweis

Die Einstellung Layer 2 Tunneling ist nur bei den folgenden Modellvarianten verfügbar:

- SCALANCE W78x im Client-Modus
- SCALANCE W746-1PRO
- SCALANCE W746-1
- SCALANCE W747-1RR
- SCALANCE W747-1

Hinweis

IP-Mapping-Tabelle

Ist bei einem Client Layer 2 Tunneling konfiguriert, wird die IP-Mapping-Tabelle nicht angezeigt.

Die Geräte SCALANCE W746-1PRO bzw. W746-1 und SCALANCE W747-1RR bzw. W747-1 sowie die im Client-Modus betriebenen Geräte SCALANCE W78x können mehreren Ethernet-Geräten den Zugang zu einem Funknetz verschaffen (IP-Mapping). Bei einem zugehörigen Access Point mit MAC-Filterung ist für den SCALANCE W700-Client nur eine

MAC-Adresse sichtbar, es kann keine Filterung nach den MAC-Adressen der Ethernet-Geräte erfolgen.

Hinweis

Mengengerüst

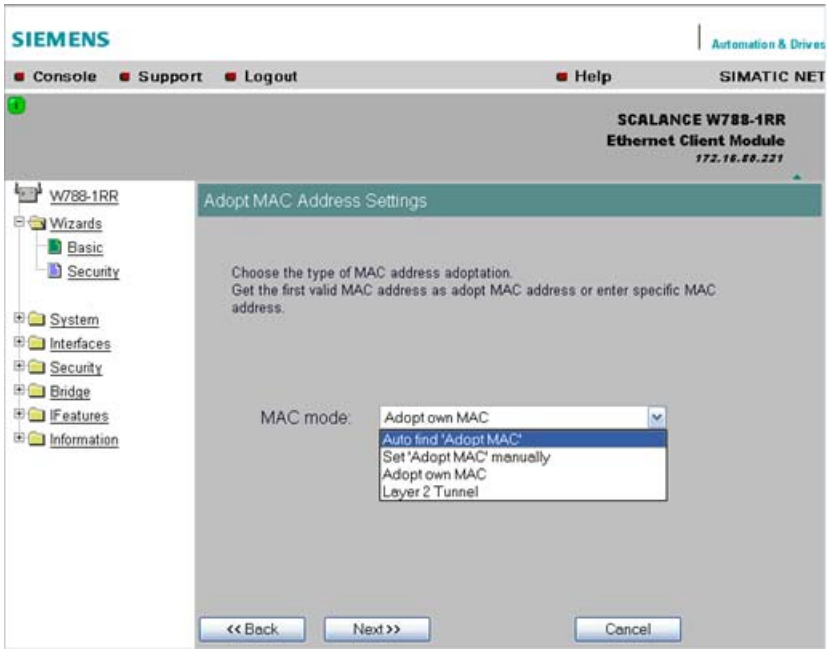
An der Ethernet-Schnittstelle eines Client Moduls werden mehrere MAC-Teilnehmer angeschlossen (z.B. PROFINET IO Geräte) und der Parameter "AdoptMAC" ist auf "Layer 2 Tunneling" eingestellt. Für eine zuverlässige Kommunikation gelten folgende Mengengerüste:

- Es dürfen nicht mehr als 8 Teilnehmer hinter dem L2T-Client angeschlossen werden.
- Beim Übertragen von zyklischen PROFINET IO-Daten im iPCF-Modus ist zu beachten, dass die Summe der Nutzdaten aller Teilnehmer am Client einen Wert von 2.300 Bytes pro Zyklus nicht überschreiten darf. Diese Angabe beinhaltet auch die Frame-Header. Ein SIMATIC-Anwender muss also neben den Netto-Daten auch die Header bei seiner Konfiguration berücksichtigen.

Klappliste *MAC mode*

Wählen Sie hier aus, wie dem SCALANCE W700-Client eine MAC-Adresse zugeordnet werden soll. Es gibt die folgenden Möglichkeiten:

- **Auto find 'Adopt MAC'**
  Der SCALANCE W700-Client nimmt automatisch die Source MAC-Adresse des ersten Telegramms an, das er über die Ethernet-Schnittstelle empfängt.
- **Set 'Adopt MAC' manually**
  Sie geben die MAC-Adresse manuell ein.
- **Adopt own MAC** (nicht beim SCALANCE W744-1PRO / W744-1)
  Der SCALANCE W700 als Client verwendet die MAC-Adresse des Ethernet Interfaces für die WLAN Schnittstelle.
- **Layer 2 Tunneling** (nicht bei SCALANCE W744 1PRO / W744-1)
  SCALANCE W700 als Client verwendet die MAC-Adresse des Ethernet Interfaces für die WLAN Schnittstelle. Zusätzlich wird das Netzwerk über die an der Ethernet-Schnittstelle des SCALANCE W700-Clients angeschlossenen MAC-Adressen informiert.



Eingabefeld *Adopt MAC*

Wenn Sie die Auswahl "Set 'Adopt MAC' manually" getroffen haben, müssen Sie hier die MAC-Adresse des Geräts eintragen, das am im Client-Modus betriebenen SCALANCE W700 über Ethernet angeschlossen ist.

Soll über den im Client-Modus betriebenen SCALANCE W700 keine Schicht 2-Kommunikation abgewickelt werden, sondern nur höhere IP-basierte Telegramme an ein oder mehrere angeschlossene Geräte gesendet werden, kann auch die Defaulteinstellung "Adopt Own Mac" ausgewählt bleiben. In diesem Modus meldet sich der Client mit der MAC-Adresse seiner Ethernet-Karte an. Die IP-Pakete werden über eine intern gehaltene Tabelle aufgeschlüsselt und an die angeschlossenen Geräte weitergeleitet.

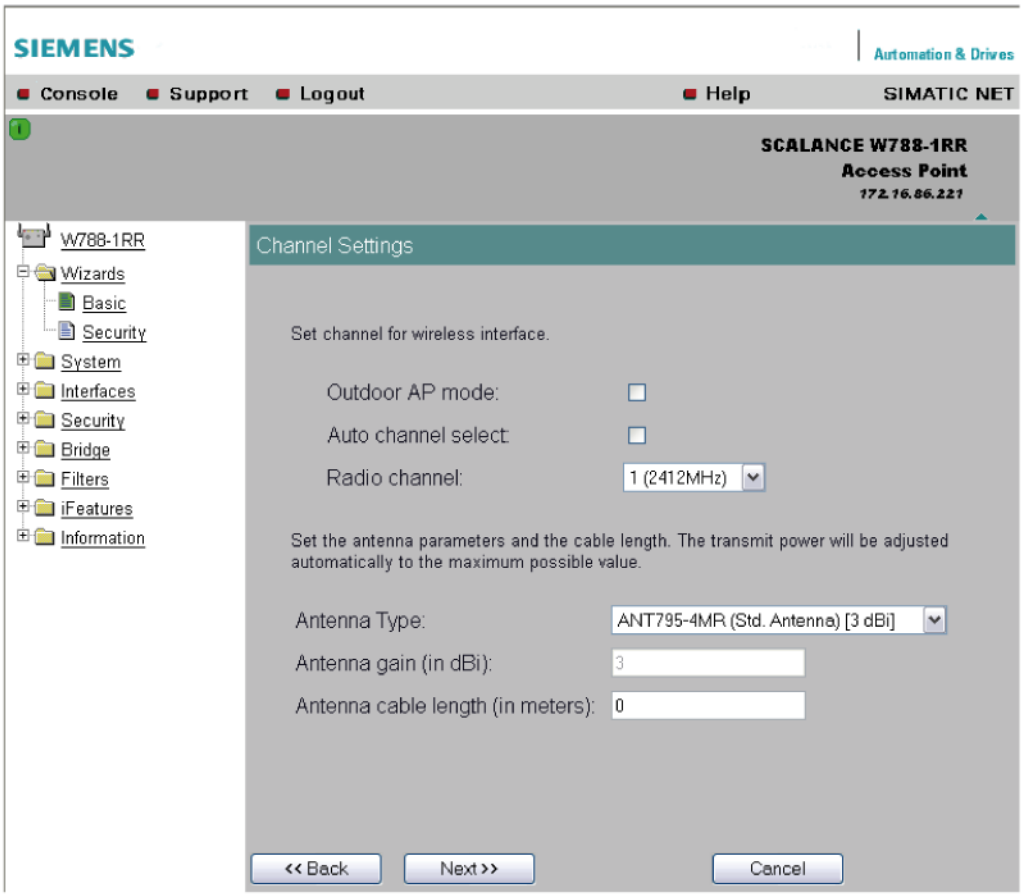
In den Betriebsmodi "Auto find 'Adopt MAC'" und "Layer 2 Tunneling" wird das Feld "Adopt MAC" ausgeblendet.

5.4.7 Kanal-Einstellungen (Nur im Access Point-Modus)

Beschreibung

Der SCALANCE W78x verwendet für die Kommunikation einen bestimmten Kanal innerhalb eines Frequenzbandes. Sie können diesen Kanal entweder fest vorgeben oder den SCALANCE W78x so konfigurieren, dass eine automatische Kanalauswahl erfolgt. Eine feste Vergabe des Kanals ist unter anderem in folgenden Situationen notwendig:

- Es gibt eine Störung der Kommunikation durch ein anderes Gerät (z. B. Mikrowellen) oder ein anderes drahtloses Netzwerk.
- Verwendung der Redundanzfunktion. In diesem Fall müssen zwei weit auseinanderliegende Kanäle oder zwei unterschiedliche Frequenzbänder gewählt werden.
- Verwendung von WDS. In diesem Fall wählen Sie einen störfreien Kanal aus, der auch vom WDS Partner benutzt wird.



Optionskästchen *Outdoor AP mode*

Markieren Sie dieses Optionskästchen, um den Outdoor AP mode zu aktivieren.

Optionskästchen *Auto Channel Select*

Markieren Sie dieses Optionskästchen, wenn Sie hinsichtlich der Kanalauswahl keine besonderen Anforderungen haben.

Klappliste *Radio Channel*

Wählen Sie hier einen für den Anwendungsfall geeigneten Kanal aus. Eine Auswahl in dieser Liste ist nur möglich, wenn das Optionskästchen "Auto Channel Select" nicht markiert ist. Der Inhalt der Auswahlliste hängt von der zuvor getroffenen Festlegung im Feld "Country code" und von der Betriebsart (IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11h) ab.

Klappliste *Antenna Type* (nur bei Geräten mit externen Antennen)

Wählen Sie den Typ der an das Gerät angeschlossenen externen Antenne aus.

Eingabefeld *Antenna gain (in dBi)* (nur bei Geräten mit externen Antennen)

Wenn Sie in der Klappliste "Antenna Type" den Eintrag "User defined" gewählt haben, können Sie manuell den Antennengewinn in der Einheit "dBi" eingeben.

Eingabefeld *Antenna cable length (in meters)* (nur bei Geräten mit externen Antennen)

Geben Sie hier die Kabellänge in Metern zwischen dem Gerät und der externen Antenne ein.

Hinweis

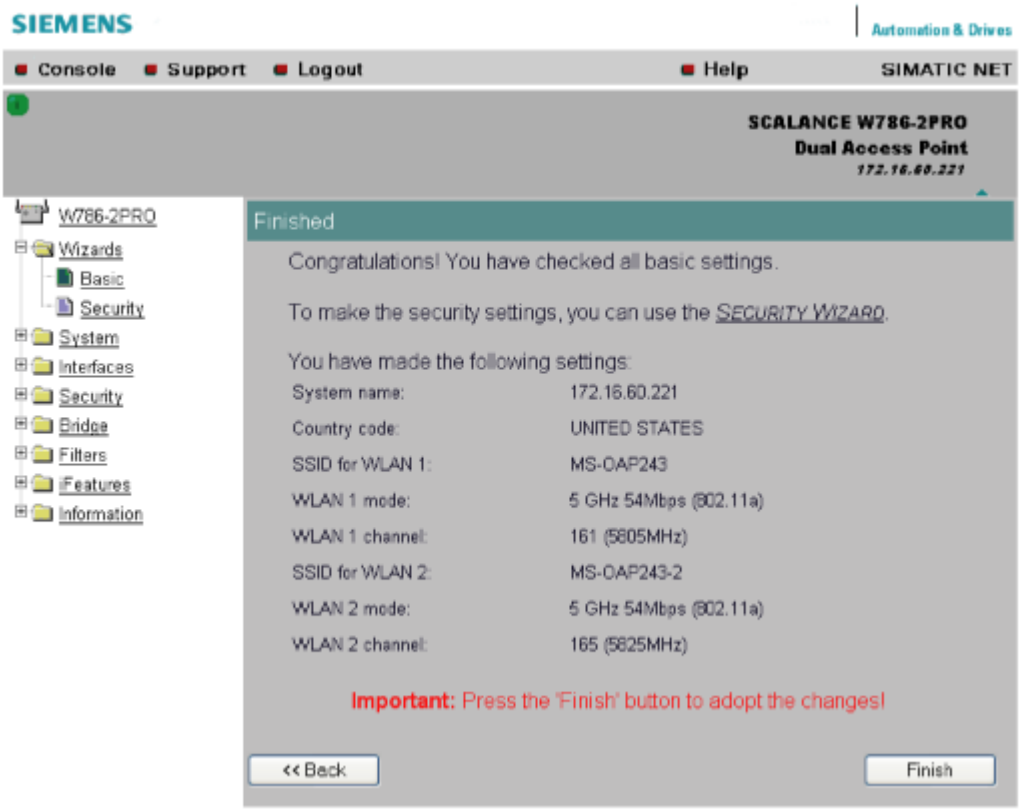
Die WLAN-Schnittstellen sind (außer beim IWLAN/PB-Link PN IO) im Auslieferungszustand deaktiviert. Diese Schnittstellen sind nutzbar, nachdem Sie den Basic Wizard durchgeführt haben.

ACHTUNG
Bei Betrieb einer zweiten oder dritten WLAN-Schnittstelle müssen Sie auf einen ausreichenden Kanalabstand achten.

5.4.8 Beenden des Basic Wizard

Beschreibung

Diese Seite zeigt die von Ihnen gewählten Parameter, wenn Sie alle Festlegungen für die Basiskonfiguration getroffen haben. Die Angabe "Adopt MAC Address" wird nur für einen Client oder für einen Access Point im Client-Modus angezeigt.



Schaltfläche *Finish*

Betätigen Sie diese Schaltfläche, um den Basic Wizard zu beenden und sich mit der geänderten IP-Adresse neu anzumelden.

5.5 Security Wizard

5.5.1 Einleitung

Der Security Wizard ermöglicht eine Festlegung sicherheitsrelevanter Parameter auch ohne Detailkenntnisse über Sicherheitstechnologien in Funknetzen.

Hinweis

Der SCALANCE W-700 kann auch ohne Konfiguration der sicherheitsrelevanten Parameter betrieben werden. Abhängig von den Eigenschaften Ihres Netzwerks besteht dann die erhöhte Gefahr eines unbefugten Zugriffs. Sie sollten deshalb alle Seiten des Security Wizards bearbeiten, um zumindest grundlegende Sicherheitsfunktionen zu nutzen.

5.5.2 Security-Einstellungen

Passwort

Vergeben Sie zunächst ein neues Admin-Passwort. Tragen Sie die gewählte Zeichenkette zweimal in die Textfelder dieser Seite ein. Das Passwort darf maximal 31 Zeichen lang sein.

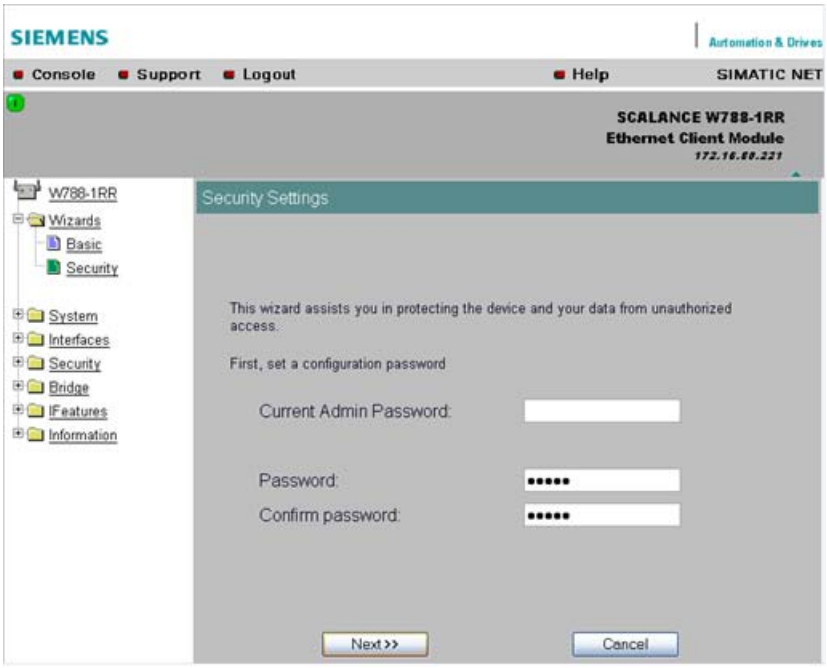
Für die Passwort-Vergabe wird der ASCII-Code 0x20 bis 0x7e verwendet. Folgende Zeichen werden unerstützt:

Die Ziffern 0...9
Die Buchstaben abcdefghijklmnopqrstuvwxyz ABCDEFGHIJKLMNOPQRSTUVWXYZ
Die Sonderzeichen !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~ und das Leerzeichen

Bis zur erstmaligen Vergabe eines Passwortes durch den Benutzer gelten die werkseitigen Voreinstellungen: Das Passwort für den Benutzer "admin" im Auslieferungszustand lautet "admin". Sie können die Wizards nur nutzen, wenn Sie als Administrator angemeldet sind.

Hinweis

Für die US-Variante des SCALANCE W-700 ist das Passwort für den Benutzer "admin" geändert, kann aber durch Fachpersonal für professionelle WLAN-Installationen beim Siemens Support erfragt werden.



5.5.3 Security-Einstellungen für die Management-Schnittstellen

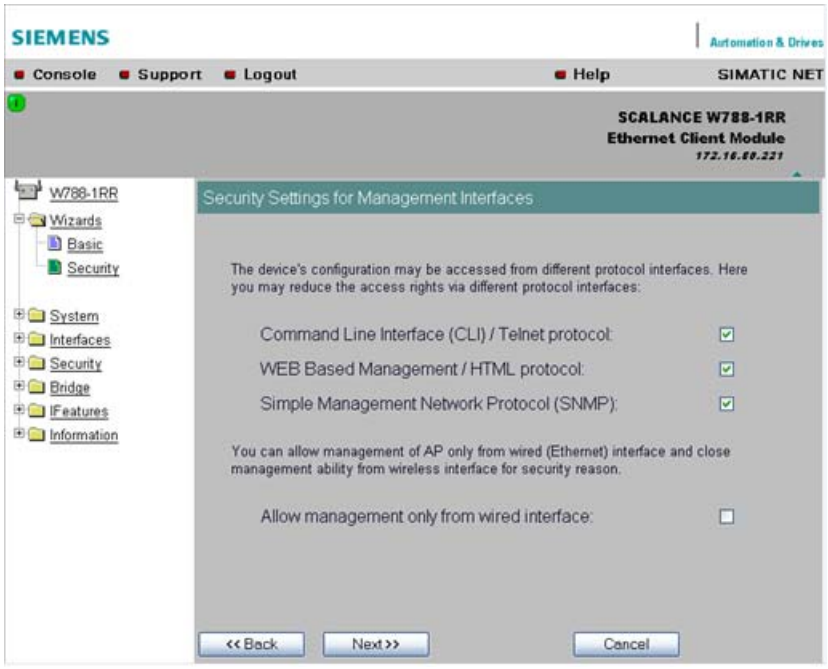
Protokolle für die Konfiguration

Auf dieser Seite legen Sie fest, über welche Protokolle Sie auf die Konfiguration des SCALANCE W-700 zugreifen. Alle Protokolle, deren Optionskästchen markiert ist, können für die Konfiguration verwendet werden. Sie sollten nur solche Protokolle auswählen, die Sie auch tatsächlich benutzen.

Die Festlegung der Protokolle wird allerdings erst nach dem Beenden des Security Wizards und einem Neustart wirksam. Sie haben also auch nach dem Markieren des Eintrags "Web Based Management" die Möglichkeit, vorhergehende Seiten zu bearbeiten oder den Wizard zu beenden.

Festlegen des Netzwerktyps für die Konfiguration

Der Zugriff auf ein drahtgebundenes Netz kann einfacher beschränkt werden als der Zugriff auf ein Funknetz. Das Web Based Management bietet die Möglichkeit, den Zugriff auf den SCALANCE W-700 zum Zweck der Konfiguration auf solche Computer zu beschränken, die über ein Kabel mit dem SCALANCE W-700 verbunden sind. Markieren Sie dazu das Optionskästchen am unteren Ende dieser Seite.

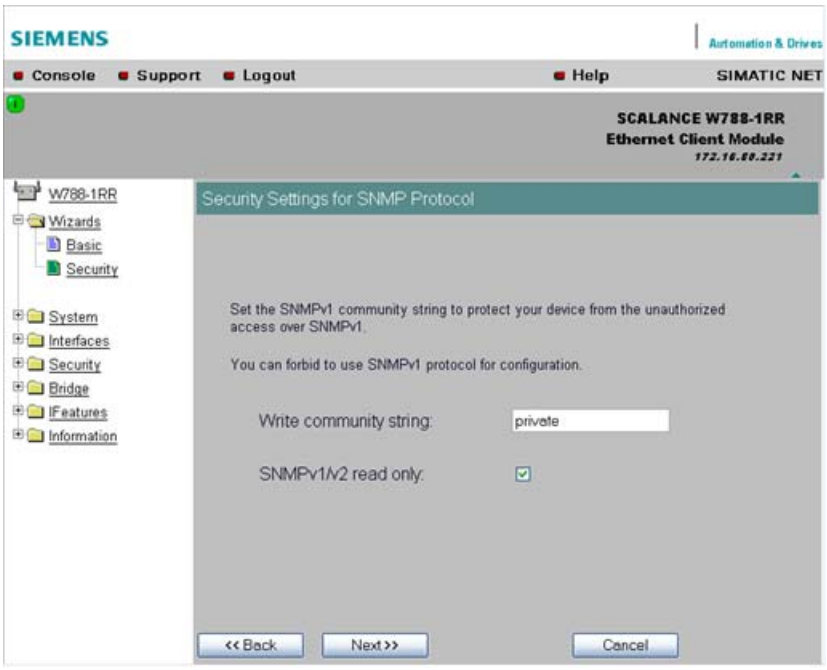


5.5.4 Security-Einstellungen für das SNMP-Protokoll

Zugriffsrechte beim SNMP-Protokoll

Die Festlegung von Zugriffsrechten beim SNMP-Protokoll erfolgt über den sogenannten Community-String. Ein Community-String vereint gewissermaßen die Aufgabe von Benutzername und Passwort in einem String; für Lese- und Schreibrechte sind verschiedene Community-Strings definiert. Erst in einigen SNMPv2-Varianten und in SNMPv3 sind komplexere und sicherere Authentifizierungen möglich.

Aus Sicherheitsgründen sollten Sie nicht die Default-Werte "public" oder "private" verwenden.



Eingabefeld *Write Community String*

Tragen Sie hier den Write Community String (maximal 63 Zeichen) für das SNMP-Protokoll ein.

Optionskästchen *SNMP Read Only*

Das Markieren dieses Optionskästchens bewirkt, dass über das SNMP-Protokoll V1 bzw. V2c nur ein lesender Zugriff möglich ist.

5.5.5 Security-Einstellungen für WLAN (Seite 1, Nur im Access Point-Modus)

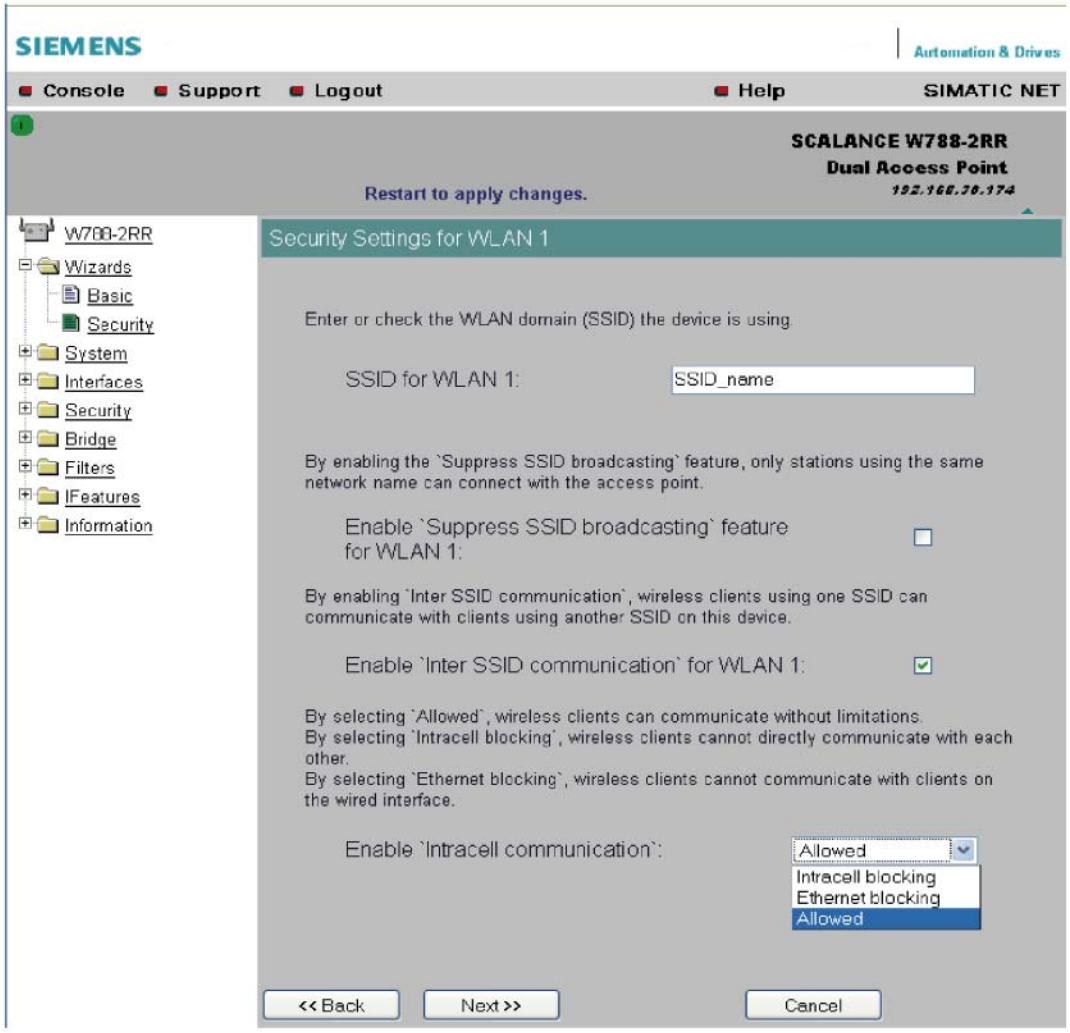
Beschreibung

Auf dieser Seite legen Sie die Sicherheitseinstellungen fest, dazu gehören beispielsweise die Authentifizierung und die Verschlüsselung. Wenn Sie ein Modell mit mehreren Funkkarten konfigurieren, erscheint diese Seite für jede Funkkarte. Sie können für jede Funkkarte unterschiedliche Einstellungen vornehmen.

Netzwerkspezifische Sicherheitseinstellungen

Auf der ersten Seite zu den Sicherheitseinstellungen treffen Sie Festlegungen, die unabhängig von protokollspezifischen Einschränkungen gelten. Grundlegende Maßnahmen zur Sicherung eines Netzwerks gegen unbefugten Zugriff bestehen darin,

- nur bestimmten Clients (solchen, die den Netzwerknamen (SSID) des APs eingetragen haben) die Kommunikation mit dem SCALANCE W78x zu ermöglichen.
- Clients, die über eine Funkverbindung kommunizieren, vom drahtgebundenen Teil des Netzwerks auszuschließen.



Eingabefeld SSID for WLAN 1

Tragen Sie in dieses Feld den Namen Ihres Netzwerks ein (maximal 255 Zeichen, 32 Zeichen bei Verwendung der Redundanzfunktion). Um mögliche Konflikte mit länderspezifischen Einstellungen auf den Computer zu vermeiden, sollte dieser Name keine deutschen Umlaute enthalten.

Option Enable 'Suppress SSID broadcasting' feature for WLAN 1

Das Markieren dieser Option bewirkt, dass die SSID für andere Geräte nicht sichtbar ist. Deshalb können sich nur solche Stationen mit dem SCALANCE W78x verbinden, bei denen der gleiche Netzwerkname wie beim SCALANCE W78x konfiguriert wurde.

Hinweis

Da bei der SSID-Übertragung keine Verschlüsselung eingesetzt wird, kann diese Funktion nur grundlegend vor unberechtigten Zugriffen schützen. Die Nutzung einer Authentifizierungsmethode (z.B. WPA (RADIUS), wenn nicht möglich WPA-PSK) bietet eine höhere Sicherheit. Es muss zudem damit gerechnet werden, dass gewisse Endgeräte Probleme mit dem Zugriff auf eine versteckte SSID haben können.

Option Enable 'Inter SSID communication' for WLAN 1

Das Markieren dieser Option erlaubt die Kommunikation zwischen WLAN-Clients, die an unterschiedlichen SSIDs eines Accesspoint angemeldet sind.

Beispiel 1	Ein SCALANCE W786-3PRO wurde mit unterschiedlichen SSIDs definiert.
Beispiel 2	Ein SCALANCE W788-1PRO wird mit Multi-SSIDs verwendet.

Hinweis

Bei einem SCALANCE W78x-2/3xx muss auf allen WLAN-Schnittstellen beziehungsweise auf allen VAPs die Funktion Inter SSID communication aktiviert werden, um eine Kommunikation zwischen den Clients mit unterschiedlichen SSIDs zu ermöglichen.

Hinweis

Wenn VLANs für die SSIDs konfiguriert sind, kann diese Einstellung die Kommunikation zwischen den SSIDs entsprechend den VLAN-Regeln verhindern.

Klappliste Enable 'Intracell communication'

- Intracell blocking
  Diese Einstellung unterbindet die Kommunikation von WLAN-Clients innerhalb einer SSID.
- Ethernet blocking
  Diese Einstellung unterbindet die Kommunikation von WLAN-Clients über die Ethernet-Schnittstelle des Accesspoint.
- Allowed
  Diese Einstellung ermöglicht sowohl die Kommunikation von WLAN-Clients innerhalb einer SSID als auch die Kommunikation von WLAN-Clients über die Ethernet-Schnittstelle.

Übersicht der Kommunikationsmöglichkeiten

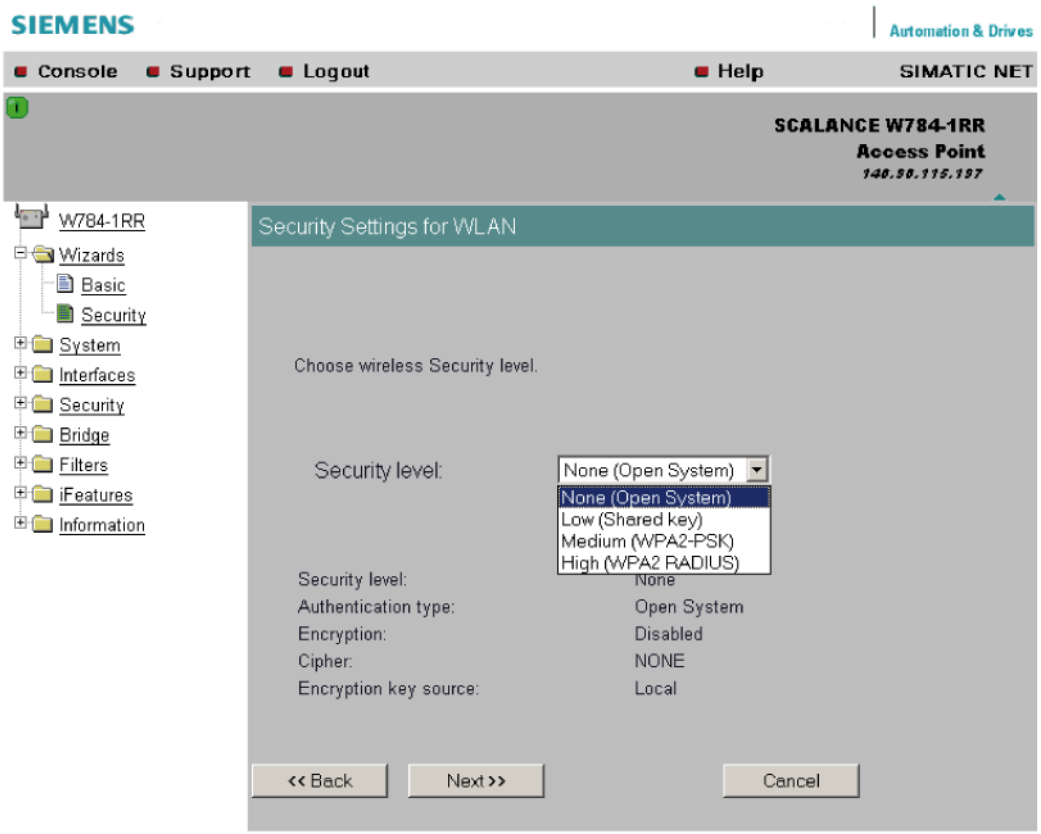
Zur Verdeutlichung finden Sie hier eine Übersicht, welche Auswirkung die beiden Einstellungen "Inter SSID communication" und "Intracell communication" haben.

Einstellungen		Mögliche Kommunikation		
Inter SSID communication	**Intracell communication**	**innerhalb einer SSID**	**zu einer anderen SSID**	**zum Ethernet-Netzwerk**
Enabled	Allowed	X	X	X
Enabled	Intracell blocking		X	X
Enabled	Ethernet blocking	X	X	
Disabled	Allowed	X		X
Disabled	Intracell blocking			X
Disabled	Ethernet blocking	X		

5.5.6 Security-Einstellungen für WLAN (Seite 2)

Vordefinierte Sicherheitsstufen

Authentifizierung und Verschlüsselung sind bewährte Maßnahmen zur Sicherung eines Netzwerks. Das Web Based Management bietet vier vordefinierte Sicherheitsstufen an, die entsprechende Methoden festlegen.



Die folgende Tabelle zeigt, was die einzelnen Sicherheitsstufen beinhalten:

Im Wizard sichtbar	Sicherheitsstufe	Authentifizierung	Verschlüsselung	Verschlüsselungsart	Schlüsselherkunft
X	None	Open System	deaktiviert	ohne	entfällt
	None	Open System	optional aktiviert	WEP	lokal
X	Low	Shared Key	aktiviert	WEP	lokal
X	Medium	WPA2-PSK (preshared Key)	aktiviert	TKIP / AES / AUTO	lokal
X	High	WPA2 (RADIUS)	aktiviert	TKIP / AES / AUTO	Server
	Medium	WPA-Auto-PSK (preshared Key)	aktiviert	TKIP / AES / AUTO	lokal
	High	WPA-Auto (RADIUS)	aktiviert	TKIP / AES / AUTO	Server

Authentifizierung

Unter Authentifizierung versteht man ganz allgemein das Erbringen eines Identitätsnachweises. Somit schützt die Authentifizierung das Netzwerk vor ungewollten Zugriffen. Im Feld "Security Level" kann zwischen folgenden Authentifizierungsarten gewählt werden:

- **None (Open System)**
  Es wird keine Authentifizierung vorgenommen. Eine Verschlüsselung mit einem festen (nicht wechselnden) Schlüssel kann optional ausgewählt werden. Hierfür müssen Sie im Menü "Keys" einen Schlüssel definieren. 5 bzw. 13 ASCII- oder 10 bzw. 26 hexadezimale Zeichen legen einen schwächeren Schlüssel (40/104 Bit) fest. 16 ASCII- oder 32 hexadezimale Zeichen definieren dagegen einen starken Schlüssel (128 Bit). Danach müssen Sie im Menü "Basic WLAN" den Punkt "Encryption" aktivieren.
- **Low (Shared Key)**
  Bei der Shared Key Authentifizierung wird im Client und Access Point ein fester Schlüssel hinterlegt. Dieser wird dann zur Authentifizierung und Verschlüsselung verwendet. Sie müssen in diesem Fall einen WEP-Schlüssel, nach der Wahl von "Low (Shared Key)", hinterlegen.
- **Medium (WPA2-PSK)**
  WPA2-PSK basiert auf dem Standard WPA2, die WPA-Authentifizierung arbeitet jedoch ohne RADIUS-Server. Statt dessen wird **auf jedem** Client und Access Point ein Schlüssel (Pass phrase) hinterlegt und zur Authentifizierung und weiteren Verschlüsselung verwendet. Als Verschlüsselungsmethode wird AES oder TKIP verwendet, AES stellt die Standardmethode dar.
- **High (WPA2)**
  WPA2 (Wi-Fi Protected Access 2) ist die Weiterentwicklung von WPA und implementiert die Funktionen des Sicherheitsstandards IEEE 802.11i. WPA2 nutzt zusätzlich das Verschlüsselungsprotokoll CCMP, das durch Vor-Authentifizierung schnelles Roaming in mobilen Ad-hoc-Netzen ermöglicht. Ein Client kann sich vorab bei mehreren Access Points anmelden, wodurch die laufende Authentifizierung entfällt.
  Zur Authentifizierung des Clients an einem Access Point wird ein RADIUS-Server genutzt. Der Client meldet sich anhand von einem Zertifikat (EAP-TLS) oder der Kombination aus Benutzername und Passwort (EAP-PEAP bzw. EAP-TTLS / innere Authentifizierungsmethode MSCHAPv2) am RADIUS-Server an. Danach weist sich der RADIUS-Server mittels Zertifikat optional gegenüber dem Client aus. Nach einer erfolgreichen Authentifizierung generieren Client und RADIUS-Server Schlüsselmaterial, das für die Datenverschlüsselung verwendet wird. Als Verschlüsselungsmethode wird AES oder TKIP verwendet, AES stellt die Standardmethode dar.
- **Medium mit WPA-Kompatibilität (WPA-Auto-PSK)**
  Wählen Sie die Sicherheitsstufe "Medium" und aktivieren Sie das Kontrollkästchen "WPA compatibility"
  Einstellung, in der ein Access Point sowohl die Authentifizierungsart "WPA-PSK" als auch "WPA2-PSK" verarbeiten kann. Dies ist erforderlich, wenn der Access Point mit verschiedenen Clients kommuniziert, die einerseits "WPA-PSK" und andererseits "WPA2-PSK" verwenden. Bei den Clients muss das gleiche Verschlüsselungsverfahren eingesetzt werden.
- **High mit WPA-Kompatibilität (WPA-Auto)**
  Wählen Sie die Sicherheitsstufe "High" und aktivieren Sie das Kontrollkästchen "WPA compatibility"
  Einstellung, in der ein Access Point sowohl die Authentifizierungsart "WPA" als auch "WPA2" verarbeiten kann. Dies ist erforderlich, wenn der Access Point mit verschiedenen Clients kommuniziert, die einerseits "WPA" und andererseits "WPA2" verwenden. Bei den Clients muss das gleiche Verschlüsselungsverfahren eingesetzt werden.

Verschlüsselung

Die Verschlüsselung schützt die zu übertragenden Daten vor Abhören und Fälschen. Sie können die Verschlüsselung im Optionskästchen "Encryption" nur dann abschalten, wenn Sie im Menü "Basic WLAN" bei der Authentifizierung "Open System" gewählt haben. Alle anderen Sicherheitsverfahren beinhalten sowohl Authentifizierung als auch Verschlüsselung. Für die Verschlüsselung werden verschiedene Verfahren eingesetzt:

- **WEP** (**W**ired **E**quivalent **P**rivacy)
  Ein schwaches symmetrisches Stromverschlüsselungsverfahren mit lediglich 40 bzw. 104 Bit langen Schlüsseln, basieren auf dem RC4-Algorithmus (Ron's Code 4).
- **TKIP** (**T**emporal **K**ey **I**ntegrity **P**rotocol)
  Ein symmetrisches Stromverschlüsselungsverfahren mit dem RC4-Algorithmus (Ron's Code 4). TKIP verwendet im Gegensatz zur schwachen WEP-Verschlüsselung wechselnde Schlüssel, die von einem Hauptschlüssel abgeleitet werden. TKIP kann außerdem gefälschte Pakete erkennen.
- **AES** (**A**dvanced **E**ncryption **S**tandard)
  Starkes symmetrisches Blockverschlüsselungsverfahren nach dem Rijndael-Algorithmus, der die Funktionen von TKIP weiter verbessert.
- **AUTO**
  Je nach Fähigkeit der Gegenstation wird TKIP oder AES verwendet.

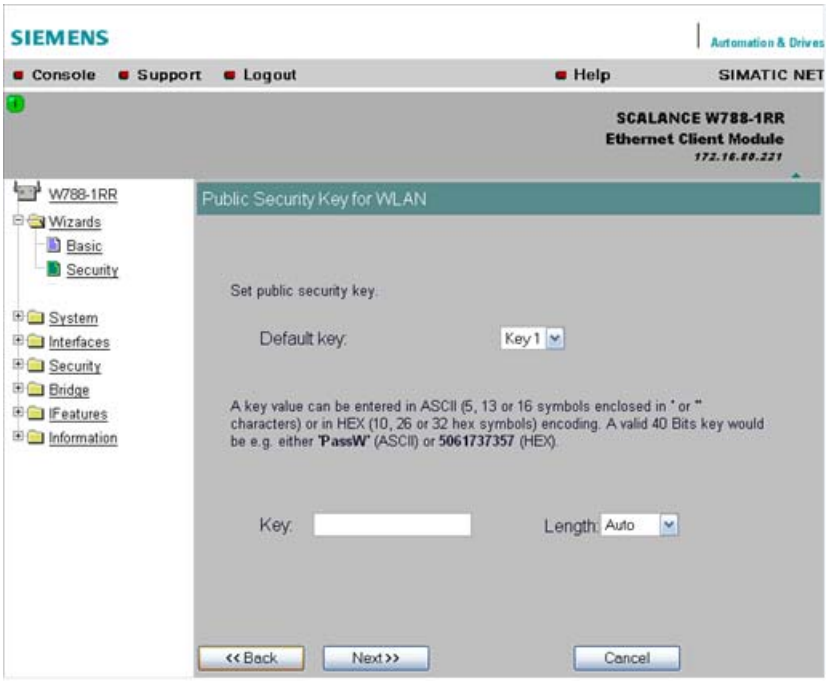
Schlüsselherkunft

Die Schlüsselherkunft gibt an, ob der Schlüssel fest konfiguriert ist (lokal), oder ob er durch ein höheres Protokoll und einen Authentifizierungsserver ausgehandelt worden ist (Server).

Klappliste *Security Level for WLAN*

Wählen Sie eine Sicherheitsstufe, die von allen Clients unterstützt wird. Der Inhalt der Folgeseite ist abhängig von der gewählten Sicherheitsstufe. Bei der Sicherheitsstufe "None" gibt es keine Folgeseite, weil in diesem Fall weder eine Verschlüsselung noch eine Authentifizierung angewendet wird.

5.5.7 Einstellungen für die Sicherheitsstufe Low



Klappliste *Default key*

Wählen Sie aus, welchen Schlüssel Sie festlegen wollen.

Eingabefeld *Key*

Tragen Sie hier die Zeichenkette für den Schlüssel ein. Sie können den Schlüssel als ASCII Zeichen oder alternativ als Hexadezimalziffer (0 – F) eingeben. Wurde der Key im ASCII Format eingetragen, wird dieser anschließend in Hochkomma dargestellt.

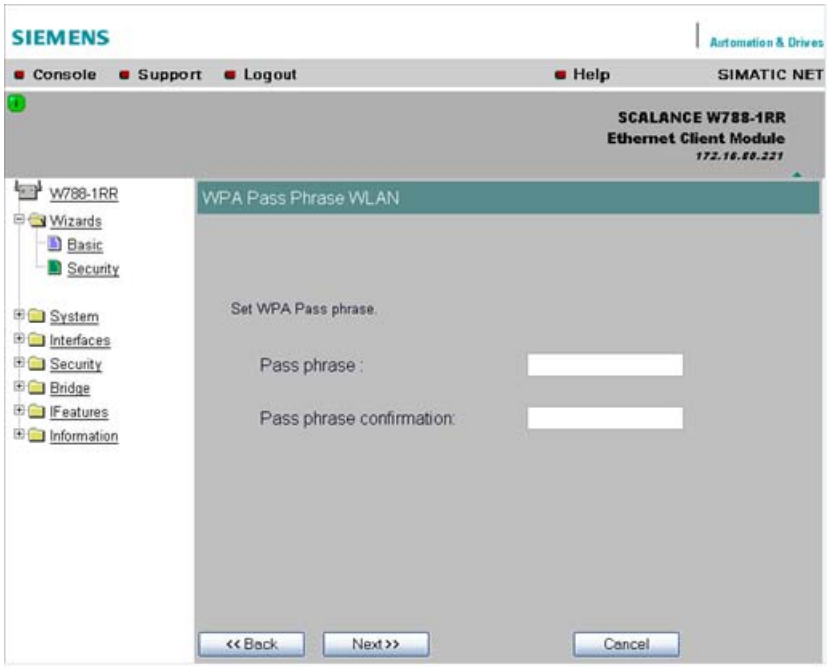
Klappliste *Length*

Wählen Sie hier aus, welche Schlüssellänge angewendet werden soll. Wenn die Länge der Zeichenkette im Eingabefeld Key größer oder kleiner als die gewählte Schlüssellänge ist, erscheint eine Fehlermeldung. Folgende Schlüssellängen sind möglich:

- 40 Bit (5 ASCII-Zeichen oder 10 Hexadezimalziffern)
- 104 Bit (13 ASCII-Zeichen oder 26 Hexadezimalziffern)
- 128 Bit (16 ASCII-Zeichen oder 32 Hexadezimalziffern)

Bei der Einstellung "AUTO" beträgt die maximale Schlüssellänge ebenfalls 128 Bit.

5.5.8 Einstellungen für die Sicherheitsstufe Medium



Eingabefeld *Pass phrase*

Geben Sie hier einen WPA2-Schlüssel ein. Der Schlüssel kann 8 bis 63 ASCII-Zeichen oder genau 64 hexadezimale Zeichen lang sein. Dieser Initialisierungsschlüssel muss sowohl auf der Client-Seite als auch dem SCALANCE W78x bekannt sein und wird vom Benutzer auf beiden Seiten eingegeben.

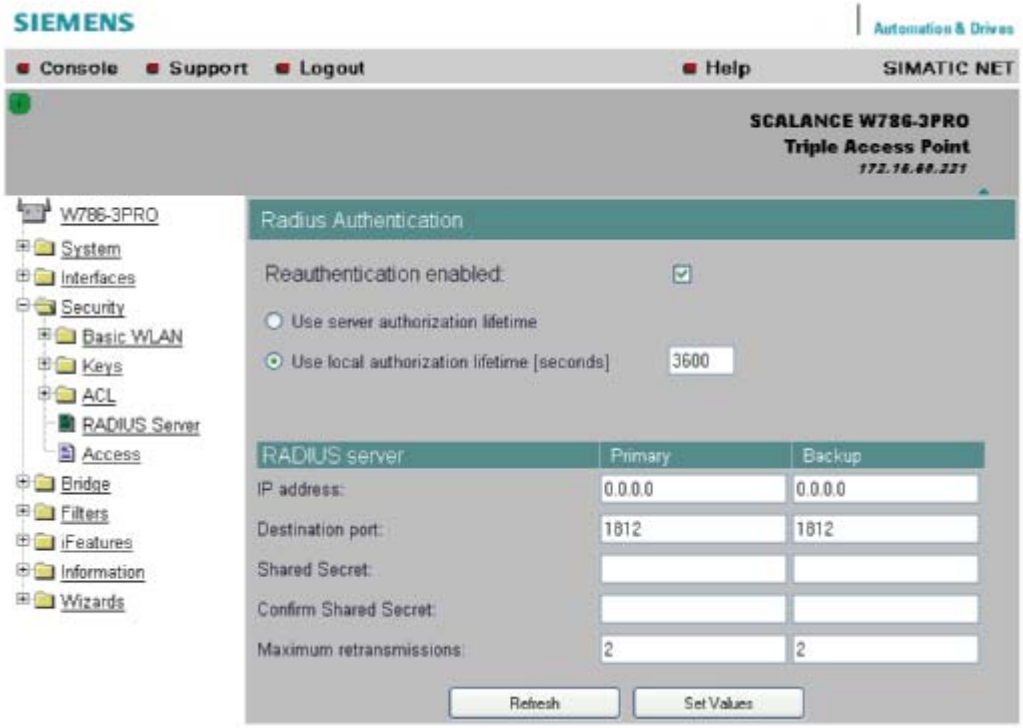
Eingabefelde *Pass phrase confirmation*

Bestätigen Sie hier den oben eingegebenen WPA2-Schlüssel.

Hinweis

Der Schlüssel kann 8 bis 63 ASCII-Zeichen oder genau 64 hexadezimale Zeichen lang sein. Er sollte komplex (z.B. aus willkürlichen Zahlen, Buchstaben (groß/klein), wenig Wiederholungen und Sonderzeichen) gewählt werden. Nutzen Sie keine bekannten Namen, Wörter oder Begriffe, die erraten werden könnten. Bei Verlust eines Gerätes bzw. bei bekannt werden des Schlüssels, sollte aus Sicherheitsgründen der Schlüssel auf allen Geräten geändert werden.

5.5.9 Einstellungen für die Sicherheitsstufe High im Access Point-Modus



Eingabefeld Reauthentication

Sie können hier einstellen, ob der Access Point eine Reauthentication für die Clients anstoßen soll. Außerdem können Sie festlegen, wer die Zeit bestimmen soll, bis die Clients zu einer neuen Reauthentication gezwungen werden. Bei der lokalen Zeitverwaltung geben Sie hier den Gültigkeitszeitraum für eine Authentifizierung in Sekunden an. Die minimale Zeitdauer beträgt 1 Minute (Eingabe 60), die maximale Zeitdauer 12 Stunden (Eingabe 43200). Der Standardwert ist eine Stunde (3.600 Sekunden).

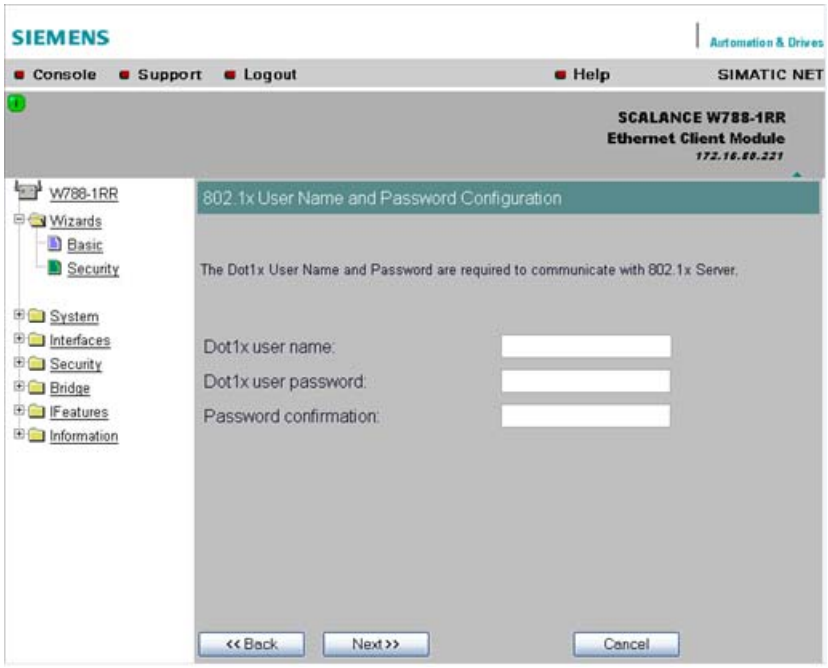
Eingabefeld RADIUS Server

Sie können die Daten für zwei RADIUS-Server eingeben, wobei die Angaben in der Spalte "Backup" verwendet werden, wenn der in der Spalte "Primary" definierte Server nicht verfügbar ist.

5.5.10 Einstellungen für die Sicherheitsstufe High für die Betriebsart "Client"

Hinweis

Die nachfolgenden Informationen gelten nur für Clients SCALANCE W74x oder Access Points SCALANCE W78x, die im Client-Modus betrieben werden.



Eingabefeld Dot1x user name

Geben Sie hier den Benutzername ein, mit dem Sie sich über den RADIUS-Server anmelden wollen.

Eingabefeld Dot1x user password

Geben Sie hier für den obengenannten Benutzername das Passwort ein. Mit dieser Kombination meldet sich der Client beim RADIUS-Server an, wenn eine Anmeldung mittels Zertifikat nicht möglich war.

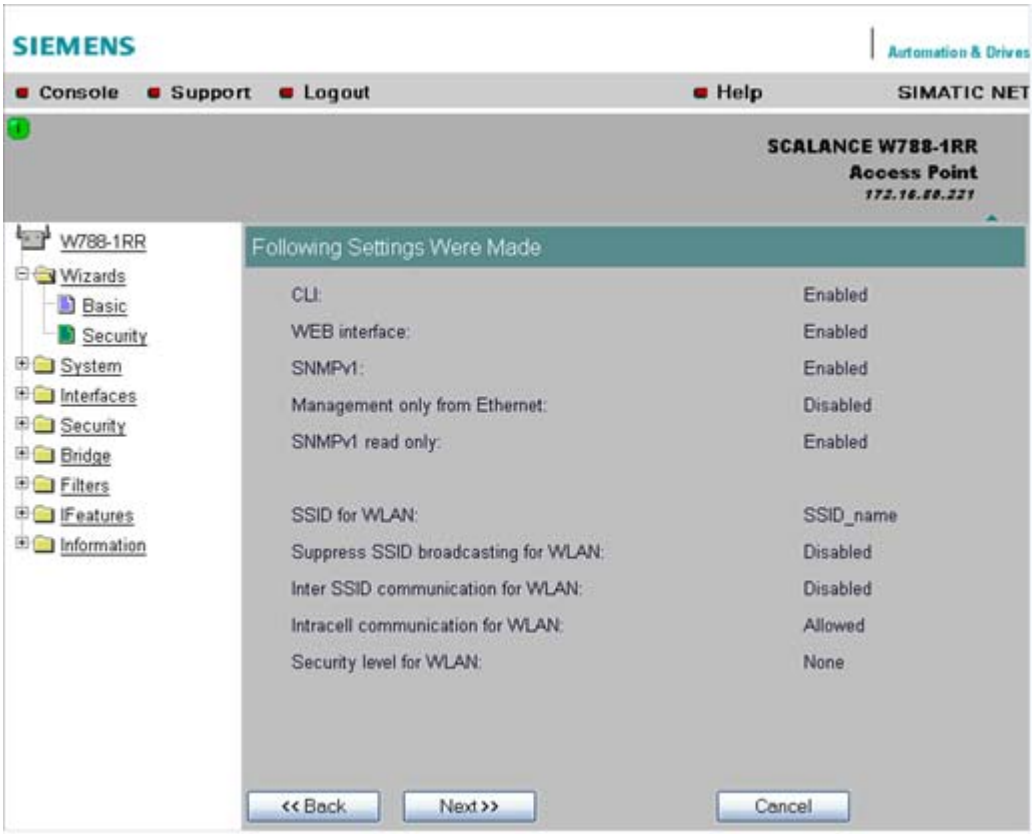
Eingabefeld Password confirmation

Bestätigen Sie hier das Passwort.

5.5.11 Übersicht der gewählten Sicherheitseinstellungen für einen Access Point

Einstellungen nach dem Bearbeiten des Security Wizards

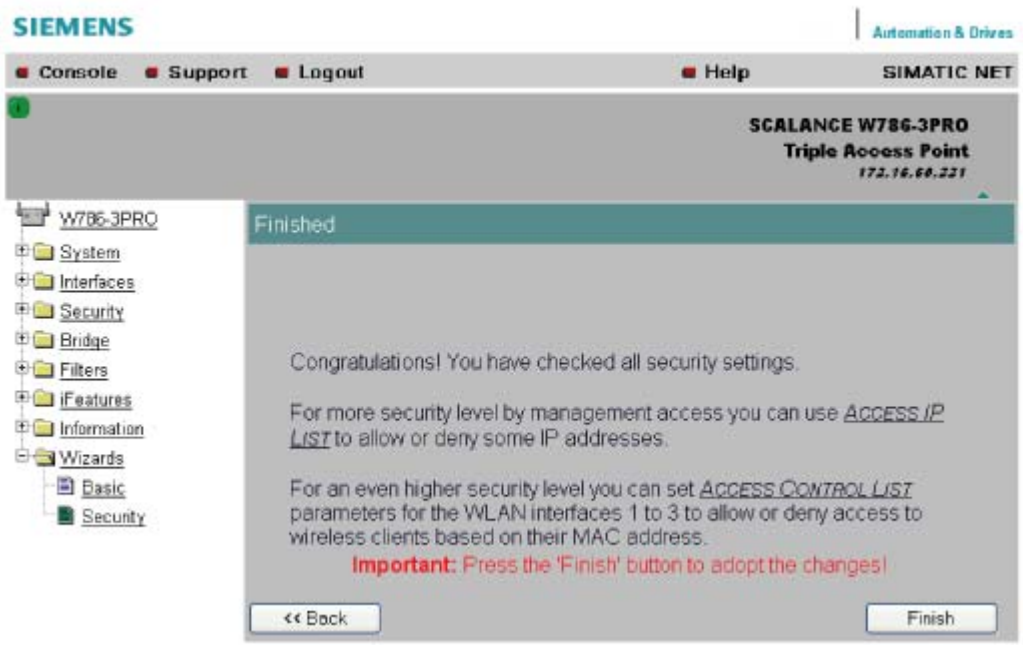
Diese Seite zeigt gewählten Sicherheitseinstellungen in einer Übersicht. Wenn Sie eine Einstellung ändern wollen, können Sie durch Anklicken der Schaltfläche "Back" zu einer der vorangegangenen Seiten gelangen und dort einen anderen Wert eingeben bzw. eine andere Auswahl treffen. Im Client-Modus enthält diese Seite weniger Informationen.



5.5.12 Beenden des Security Wizards

Weitergehende Sicherheitseinstellungen

Die letzte Seite des Wizards weist auf weitergehende Sicherheitseinstellungen hin.



Schaltfläche *Finish*

Klicken Sie die Schaltfläche Finish, um die Daten zu übernehmen und den Wizard zu beenden. Damit die vorgenommenen Einstellungen wirksam werden, müssen Sie einen Neustart durchführen (Menü **System > Restart**).

5.6 Konfiguration über das Web Based Management

5.6.1 Allgemeine Informationen zum Web Based Management

Navigationsleiste

In der oberen Menüleiste des Web Based Managements (WBM) befinden sich folgende Links:

- Console
  Dieser Link öffnet ein Konsolen-Fenster, in dem Sie CLI-Befehle eingeben können.
- Support
  Durch Anklicken dieses Links rufen Sie eine Support-Seite der SIEMENS AG im Internet auf.
- Logout
  Beenden Sie die aktuelle Sitzung des Web Based Managements durch Anklicken dieses Links. Es wird dann wieder die Anmeldemaske angezeigt.
- Help
  Wenn Sie diesen Link anklicken, öffnet sich die Onlinehilfe des Web Based Managements in einem eigenen Browserfenster.

Aktualisieren der Anzeige mit Refresh

Seiten des Web Based Managements, die aktuelle Parameter anzeigen, haben am unteren Rand die Schaltfläche "Refresh". Klicken Sie diese Schaltfläche, wenn Sie für die angezeigte Seite aktuelle Daten vom Gerät anfordern wollen.

Speichern von Einträgen mit Set Values

Seiten, auf denen Sie Konfigurationsdaten festlegen können, haben am unteren Rand die Schaltfläche "Set Value". Klicken Sie diese Schaltfläche, um eingegebene Konfigurationsdaten im Gerät zu speichern.

Anlegen von Einträgen mit NEW

Seiten, auf denen Sie Listen erstellen können, haben am unteren Rand die Schaltfläche "New". Klicken Sie diese Schaltfläche, um einen neuen Eintrag in der Liste zu erstellen.

Zurücksetzen des Zählers mit Reset Statistics

Mit dieser Schaltfläche können Sie die entsprechenden Zähler zurücksetzen.

Hinweis zum Login User

Falls Sie sich als User anmelden, wird ihnen nur ein eingeschränktes WEB und Telnet zu Verfügung stehen. Da Sie nur Lesezugriff haben, sind unter Telnet einige Befehle nicht vorhanden und einige Bereiche nicht auswählbar.

Vorausgesetzte Kenntnisse

Um die Informationen dieses Kapitels sinnvoll umsetzen zu können, sollten Sie Detailkenntnisse über die Netzwerk-Technologie und WLAN haben.

5.6.2 Leuchtdiodensimulation des Web Based Management

Darstellung des Betriebszustands

Der SCALANCE W-700 verfügt über mehrere Leuchtdioden, die Informationen über den Betriebszustand des Geräts liefern. Abhängig vom Aufstellungsort ist der direkte Zugang zum SCALANCE W-700 jedoch nicht immer möglich. Aus diesem Grund bietet das Web Based Management eine Simulationsdarstellung für die Leuchtdioden.

Aktivieren der Simulationsdarstellung

Es gibt eine HTML-basierte Simulationsdarstellung des Leuchtdiodenzustands. Klicken Sie auf das grüne Icon unter dem Link Console, um die Simulationsdarstellung zu aktivieren.

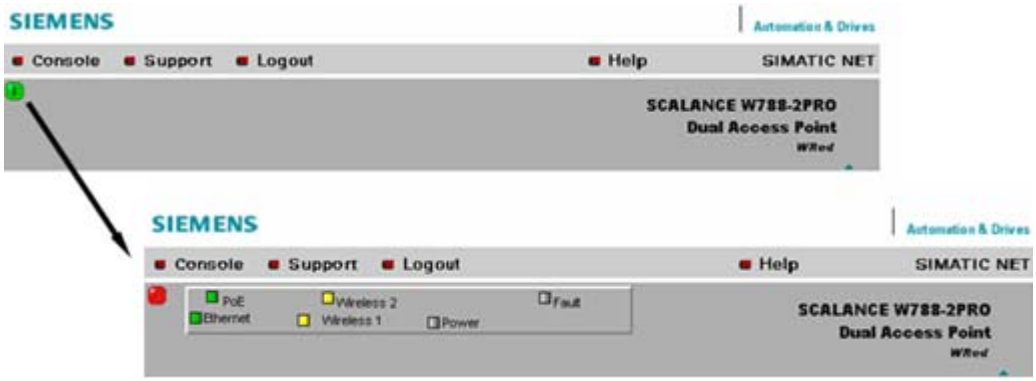


Bild 5-1 Beispiel: Leuchtdiodenanzeige eines SCALANCE W788-2PRO. Andere Gerätevarianten haben eine davon abweichende Darstellung der Leuchtdioden.

5.6.3 Das Menü System

5.6.3.1 Menüpunkt System Information

Betriebsart und Ländereinstellung

Auf dieser Seite machen Sie einige grundlegende Einstellungen für den SCALANCE W-700, beispielsweise die Ländereinstellung und die Festlegung der Betriebsart (Access Point oder Client).

Wechsel der Betriebsart bei Access Points

Beim Umschalten vom Access Point-Modus in den Client-Modus und zurück werden alle Parameter gelöscht außer:

- IP-Adresse
- Subnetz-Maske
- Gateway-Adresse
- SSID (nur im Access Point Modus)
- IP-Adresse des Default-Routers
- DHCP-Flag
- System Name
- System Location
- System Contact
- Device Mode
- Country Code
- User und Admin Kennwörter

Das Ausgabefeld "Current system time" informiert über die Systemzeit. Das Ausgabefeld "System up time" informiert über die abgelaufene Zeitdauer seit dem letzten Neustart ("Restart").

Auslesen der Country List

Geben Sie im Adressfeld des Internet-Browsers
`https://<IP-Adresse des SCALANCE W-700>/countrylist.log`

ein und bestätigen Sie mit "Enter".

Sie erhalten nach dem Einloggen die Country List mit den folgenden Rubriken:

```
-----------------------------------------------------------------
COUNTRY      |   MODE   |   CH   |   MHz   |   PWR(EIRP)   |   USAGE
-----------------------------------------------------------------
```

Die Tabelle enthält für jede mögliche Ländereinstellung die zulässigen Funkmodi und Kanäle und die zugehörigen Kanalfrequenzen. Die Rubrik PWR(EIRP) beinhaltet die zulässigen Grenzwerte für die Sendeleistung, gemessen an der Antenne. Die Grenzwerte beziehen sich auf die Sendeleistung des Access Point und den Antennengewinn der eingesetzten Antenne.

Hinweis

Bei der Ausführung für USA können Sie keine Länderauswahl durchführen. Die für dieses Land geeigneten Frequenzbänder sind bereits fest voreingestellt.

5.6.3.2 Menüpunkt IP Einstellungen

Konfiguration

Wählen Sie hier aus, ob Sie einen DHCP-Server verwenden wollen oder ob Sie dem SCALANCE W-700 eine feste IP-Adresse zuweisen wollen. Darüber hinaus können Sie die IP-Adresse eines Routers und die Default-TTL einstellen. Der Parameter TTL (Time to live) gibt die maximale Anzahl Router an, die ein Datenpaket überwindet, bevor es verworfen wird.

Hinweis

Wenn Sie einen Radius-Server zur Authentifizierung verwenden, muss dieser über das Management VLAN erreichbar sein.

Siehe auch

- Menüpunkt CLI\SYSTEM\IP (Seite 199)

5.6.3.3 Menüpunkt Services

Konfiguration

Wählen Sie hier aus, über welche Dienste ein Zugriff auf das Gerät möglich sein soll. Ist beispielsweise das Optionskästchen "SNMP Enabled" nicht markiert, so ist weder ein schreibender noch ein lesender Zugriff über das SNMP-Protokoll (v1,v2c,v3) möglich. Falls

das SNMP – Protokoll nicht zugelassen ist, dann ist auch das Versenden von SNMP-Traps nicht möglich.

Aus Sicherheitsgründen sollten Sie nur solche Dienste aktivieren, die Sie auch tatsächlich nutzen.

ACHTUNG
Über SNMP ist es möglich, alle Dienste zu deaktivieren und über SNMP nur den Lesezugriff zu ermöglichen. Danach ist keine weitere Konfiguration des Geräts mehr möglich.

Wenn Sie zum Konfigurieren des Gerätes nur den sicheren Zugriff über HTTPS aktivieren wollen, dann markieren Sie das Optionskästchen "HTTPS only".
Wenn Sie das Antworten des Gerätes auf Ping-Signale ermöglichen wollen, dann markieren Sie das Optionskästchen "Ping enabled".

Über den eingebauten SSH-Server erhalten Sie einen gesicherten Zugriff auf das CLI. Im Gegensatz zu Telnet läuft hierbei die gesamte Kommunikation inklusive der Benutzerauthentifizierung verschlüsselt ab.

Anmerkungen zu WEB Enabled im WEB-Interface

Das Optionskästchen zum Eintrag "WEB Enabled" ist markiert und inaktiv gesetzt, weil ohne Zugriffsmöglichkeit über HTTP natürlich keine Konfiguration mit dem Web Based Management mehr möglich ist.

Wenn Sie die Konfigurationsmöglichkeit über das Web Based Management abschalten wollen, können Sie das mit dem Security Wizard oder über Telnet und SNMP tun. Dort über Security Wizard vorgenommene Einstellungen werden erst nach einem Neustart des Geräts wirksam.

Siehe auch

- Menüpunkt CLI\SYSTEM\SERVICES (Seite 200)

5.6.3.4 Menüpunkt Restart

Schaltfläche *Restart*

Klicken Sie auf diese Schaltfläche, um das Gerät neu zu starten. Bei einem Neustart wird das Gerät neu initialisiert, die interne Firmware wird neu geladen und das Gerät führt einen Selbsttest durch. Die gelernten Einträge in der Adresstabelle werden gelöscht. Sie können das Browser–Fenster geöffnet lassen, während das Gerät neu startet.

Schaltfläche *Restore Memory Defaults*

Klicken Sie diese Schaltfläche, um die Konfiguration zurückzusetzen. Dabei werden die folgenden Parameter (geschützten Voreinstellungen) nicht zurückgesetzt:

- IP-Adresse
- Subnetz-Maske
- Gateway-Adresse
- SSID
- IP-Adresse des Default-Routers
- DHCP-Flag
- System Name
- System Location
- System Contact
- Device Mode
- Country Code

Es wird kein automatischer Neustart ausgeführt, damit Sie zuvor noch Daten über das Web Based Management eingegeben können. Die Änderungen werden erst wirksam, wenn Sie einen Neustart durchführen.

Wenn Sie als User angemeldet sind, ist die Schaltfläche "Restore Memory Defaults" nicht sichtbar.

Schaltfläche *Restore Factory Defaults and restart*

Klicken Sie auf diese Schaltfläche, um die werkseitigen Konfigurationseinstellungen wiederherzustellen. Es werden auch die geschützten Voreinstellungen (siehe oben) zurückgesetzt. C-PLUG wird neu initialisiert und formatiert, falls vorhanden. Es wird ein automatischer Neustart ausgeführt.

Hinweis

Durch das Zurücksetzen aller Voreinstellungen geht auch die IP-Adresse verloren. Das Gerät ist danach nur über das Primary Setup Tool ansprechbar, falls die Vergabe einer IP-Adresse nicht über DHCP erfolgt.

Wenn Sie als User angemeldet sind, ist die Schaltfläche "Restore Factory Defaults" nicht sichtbar.

Siehe auch

- Menüpunkt CLI\SYSTEM\RESTARTS (Seite 201)

5.6.3.5 Menüpunkt Event Config

Systemereignisse des Geräts

Auf dieser Seite legen Sie fest, wie das Gerät auf Systemereignisse reagiert. Sie können für folgende Ereignisse die Reaktion des SCALANCE W-700 konfigurieren:

- Start des Geräts

- Änderung des Ethernet Status Link up / Link down
- Fehler beim Einloggen eines Benutzers
- Änderung der Energieversorgung des Geräts (Eine Auswertung dieses Ereignisses ist nur bei redundanter Spannungsversorgung sinnvoll.)
- Änderung des Fehlerstatus (Fehler-LED)

Zusätzliche Systemereignisse für Access Points

Wenn Sie einen SCALANCE W78x im Access Point-Modus einsetzen, können Sie zusätzliche Systemereignisse konfigurieren:

- Ereignisse im Zusammenhang mit dem An- und Abmelden eines Client
- IP-Alive State Change (Applikationsspezifische Verbindungsüberwachung)
- Link Check State Change (Gerätespezifische Verbindungsüberwachung)
- Ereignisse im Zusammenhang mit der Bandbreitenreservierung iQoS
- Erkennung von Access Points auf dem eigenen oder einem überlappenden Funkkanal
- Topologie-Änderungen bei Rapid Spanning Tree
- Bei den Gerätevarianten SCALANCE W78x-xRR Ereignisse im Zusammenhang mit iPCF
- Ereignisse im Zusammenhang mit der Funktion Forced Roaming on IP down
- Änderung des WDS-Verbindungsstatus Link up / Link down

Bei den Gerätevarianten mit mehr als einer WLAN-Schnittstelle gibt es außerdem den Zustand der Redundanzverbindung (redundant, nicht redundant, unterbrochen) als Systemereignis.

Reaktion auf Systemereignisse

Es gibt folgende Alternativen, wie das Gerät auf ein Systemereignis reagieren kann:

- Das Gerät sendet eine E-Mail.
- Das Gerät löst eine SNMP-Trap aus.
- Das Gerät schreibt einen Eintrag in die Log-Datei.
- Das Gerät löst einen Fehler aus (die Fehler-LED leuchtet auf).

Durch Markieren der entsprechenden Optionskästchen legen Sie fest, bei welchen Ereignissen welche Reaktionen des Geräts erfolgen sollen. Mit den Optionskästchen in der Zeile "Functions enabled" aktivieren bzw. deaktivieren Sie das Versenden von E-Mails bzw. das Auslösen von SNMP-Traps.

5.6.3.6 Menüpunkt E-Mail Config

Absender und Empfänger einer E-Mail

Hier legen Sie fest, an wen das Gerät bei entsprechend konfigurierten Ereignissen eine E-Mail sendet. Außerdem können Sie einen Absender eintragen. So können Sie bei Benachrichtigungen erkennen, welches Gerät betroffen ist. Wenn Sie im Feld "From" keine Eintragung vornehmen, verwendet das Gerät folgenden Absender: SCALANCE_W@<IP-Adresse>

Siehe auch

- Menüpunkt CLI\SYSTEM\EMAIL (Seite 205)

5.6.3.7 Menüpunkt SNMP Config

Konfiguration

Markieren Sie die Optionskästchen der Einträge abhängig von der SNMP-Funktionalität, die Sie nutzen wollen. SNMP Version 3 bietet eine Rechtevergabe auf Protokollebene, Authentifizierung und Verschlüsselung. Die Festlegung von Gruppen und Benutzern erfolgt in den Untermenüs Groups und Users. Sie können dort auch dann Eingaben machen, wenn Sie das Optionskästchen SNMPv3 enabled nicht markiert haben, allerdings werden die Eintragungen dann nicht angewendet.

ACHTUNG
Bei der Verwendung von SNMP Version 3 sollten Sie SNMP V1 und V2c deaktivieren, weil die Sicherheitseinstellungen von SNMP V3 durch einen Zugriff über SNMP V1 oder V2c unterlaufen werden können.

Untermenüpunkt *Trap*

Tragen Sie hier die IP-Adressen von bis zu 10 Trap-Empfängern ein. Das Gerät versendet eine Trap an alle eingetragenen Adressen, bei denen das Optionskästchen Enable Trap markiert ist.

Hinweis

Bei Warmstart / Kaltstart ist bei Wireless Verbindung (AP-Client, WDS oder WRED) nicht gewährleistet, dass zum Zeitpunkt des Sendens der Trap der Empfänger erreichbar ist. Hierdurch kommt es zum Verlust der Meldung.

Untermenüpunkt *Groups*

Diese Seite zeigt die SNMPv3-Gruppen an. Sie legen eine neue Gruppe an, indem Sie die Schaltfläche "New" anklicken und den Gruppennamen, die Sicherheitsstufe und die Berechtigung zum Schreiben bzw. zum Lesen festlegen.

Sie löschen eine Gruppe, indem Sie das Optionskästchen in der Spalte "Del" markieren und die Schaltfläche Set "Values" anklicken. Falls in der Gruppe bereits Mitglieder eingetragen sind, können Sie die Gruppe nicht löschen und auch eine Veränderung der Sicherheitsstufe der Gruppe nicht möglich.

Es gibt drei SNMPv3 Sicherheitsstufen:

Sicherheitsstufe	Besonderheiten	Kommentar
None	Keine Authentifizierung, keine Verschlüsselung.	
Auth/No Priv	Authentifizierung mit dem MD5 oder SHA-Algorithmus, keine Verschlüsselung.	Um die Mitglieder einer Gruppe anzuzeigen, muss man das Authentifizierungskennwort (max. 63 Zeichen) eingeben.
Auth/Priv	Authentifizierung mit dem MD5 oder SHA-Algorithmus, Verschlüsselung mit dem DES3 Algorithmus.	Um die Mitglieder einer Gruppe anzuzeigen, muss man das Authentifizierungskennwort (max. 63 Zeichen) eingeben.

Untermenüpunkt *Users*

Diese Seite zeigt die SNMPv3-Benutzer an. Sie legen einen neuen Benutzer an, indem Sie die Schaltfläche "New" anklicken und den Benutzernamen und die Gruppe festlegen, der der Benutzer angehören soll. Falls nötig, müssen Sie noch die Kennwörter für die Authentifizierung und für die Verschlüsselung eingeben.

Sie löschen einen Benutzer, indem Sie das Optionskästchen in der Spalte "Del" markieren und die Schaltfläche "Set Values" anklicken.

Siehe auch

- Menüpunkt CLI\SYSTEM\SNMP (Seite 206)
- Menüpunkt CLI\SYSTEM\SNMP\GROUP (Seite 207)
- Menüpunkt CLI\SYSTEM\SNMP\USER (Seite 209)

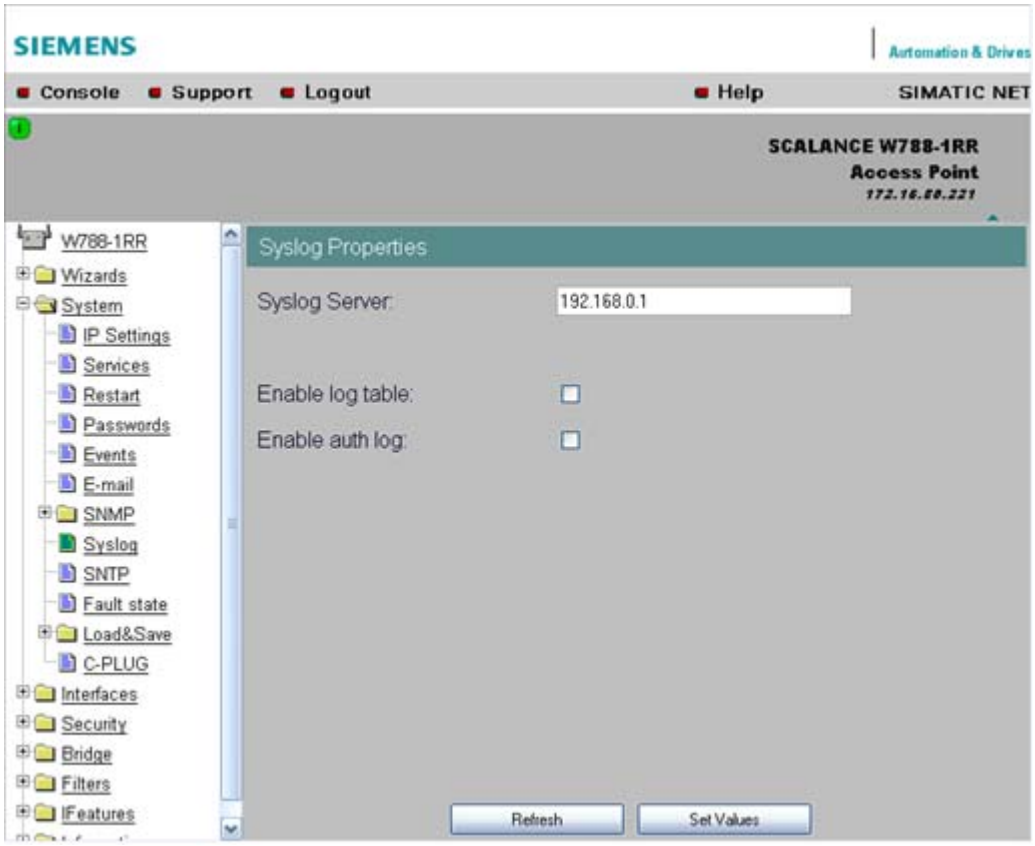
- Menüpunkt CLI\SYSTEM\SNMP\TRAP (Seite 210)

5.6.3.8 Menüpunkt Syslog

Syslog nach RFC 3164 wird für die Übermittlung von kurzen, unverschlüsselten Textmeldungen per UDP im IP-Netz verwendet. Dazu wird ein Standard-Syslog-Server benötigt.

Syslog-Konfiguration beim SCALANCE W-700

Die für das Syslog-Protokoll verwendeten Parameter werden im Menüpunkt **System -> Syslog** angezeigt und eingestellt:



Die Parameter haben folgende Bedeutung:

Eingabefeld Syslog Server

Die Server Adresse bestimmt an welche IP-Adresse die Syslog- Nachrichten geschickt werden. Ist in diesem Feld keine IP- Adresse eingetragen, werden keine Syslog-Nachrichten versendet. Befindet sich der Syslog-Server nicht im gleichen Netz wie der Scalance W wird automatisch versucht, über das Default Gateway eine Verbindung aufzubauen.

Optionskästchen log table

Anhand dieser Checkbox wird festgelegt ob alle Einträge die in die Log Table gemacht werden auch als Syslog- Nachricht verschickt werden.

Optionskästchen auth log

Anhand dieser Checkbox wird festgelegt ob alle Einträge die in das Authentication Log gemacht werden auch als Syslog- Nachricht verschickt werden.

Siehe auch

- Menüpunkt CLI\SYSTEM\SYSLOG (Seite 211)

5.6.3.9 Menüpunkt SNTP Config

Zeitsynchronisation im Netzwerk

SNTP ist die Abkürzung für Simple Network Time Protocol. Ein Server nutzt dieses Protokoll, um im gesamten Netzwerk eine einheitliche Zeit zur Verfügung zu stellen. Clients können sich mit dieser Zeit synchronisieren.

Wenn Sie im Textfeld "SNTP server" die IP-Adresse eines SNTP-Servers eingeben und im Auswahlfeld "Time zone offset" die Zeitzone des SCALANCE W-700 auswählen, nutzt der SCALANCE W-700 die Zeitinformation dieses Servers. Der SCALANCE W-700 übernimmt diese Zeitinformation ohne weitere Umrechnung bezüglich Sommer- und Winterzeit.

In Textfeld "Update interval" geben Sie die Zyklusdauer in Sekunden an, nach der der SCALANCE W-700 beim SNTP-Server die Zeitinformation abruft. Mit der Schaltfläche "Refresh SNTP" können Sie einen Abgleich mit dem SNTP-Server unabhängig von der eingestellten Zykluszeit vornehmen.

Siehe auch

- Menüpunkt CLI\SYSTEM\SNTP (Seite 212)

5.6.3.10 Menüpunkt Fault State

Informationen über Fehler

Diese Seite zeigt Informationen über aufgetretene Fehler. Sie können diese Informationen löschen, wenn Sie die Schaltfläche "Remove Fault State" anklicken.

Siehe auch

- Menüpunkt CLI\SYSTEM\FAULT (Seite 213)

5.6.3.11 Menüpunkt Load & Save

Speichern und Laden von Gerätedaten

Nach Anklicken des Menüpunkts Load & Save erscheint zunächst eine Seite, die die aktuelle Firmware-Version anzeigt. Die Untermenüpunkte "HTTP" und "TFTP" bieten die Möglichkeit, Gerätedaten in externen Dateien zu speichern bzw. aus externen Dateien in das Gerät zu übernehmen. Wird das Gerät mit C-PLUG betrieben, dann werden die Daten der geladenen Konfigurationsdatei auf dem C-PLUG gespeichert. Solange der C-PLUG gesteckt ist, arbeitet das Gerät mit der Konfiguration auf dem C-PLUG.

Sie können folgende Gerätedaten in externen Dateien speichern:

- die Konfigurationsdaten des Geräts
- den Inhalt der Log-Tabelle
- die Firmware des Geräts
- das Client-Zertifikat (nur bei Clients und Access Points im Client Modus)
- das Server-Zertifikat (nur bei Clients und Access Points im Client Modus)

Sie können folgende Daten aus externen Dateien in das Gerät übernehmen:

- die Konfigurationsdaten des Geräts
- die Firmware des Geräts
- das Client-Zertifikat (nur bei Clients und Access Points im Client Modus)
- das Server-Zertifikat (nur bei Clients und Access Points im Client Modus)

Weitere Informationen über Zertifikate entnehmen Sie bitte dem "Systemhandbuch Grundlagen Industrial Wireless LAN".

Hinweis

Beim Laden von Konfigurationsdaten auf das Gerät wird ein Neustart ausgeführt, damit die neuen Daten richtig übernommen werden. Der Neustart wird beim HTTP- und TFTP-Ladevorgang automatisch durchgeführt. Das Gerät ist unter der alten IP-Adresse nicht mehr erreichbar, falls in den geladenen Konfigurationsdaten eine neue IP-Adresse vorhanden ist.

Hinweis

Nur für SCALANCE W788-xPRO/RR und W74x-1PRO/RR

Ab FW-Stand V3.0 enthält die Datei mit den Konfigurationsdaten des APs zusätzlich noch folgende Information

- Version der Konfigurationsdatei
- FW-Version, mit der diese Konfigurationsdatei erzeugt wurde
- MLFB-Nummer des Geräts, mit dem die Konfigurationsdatei erzeugt wurde

Die auf dem C-PLUG vorhandene Konfiguration muss mit einem FW-Stand ≤ dem FW-Stand auf dem Zielgerät erzeugt worden sein.

Beispiel:

Konfigurationsdateien, die mit einem Gerät der Firmware V2.4 oder älter erzeugt wurden, können problemlos in Geräte mit dem Firmware-Stand V3.0 (bzw. V3.2 beim W786-xPRO und V3.3 beim W784-1xx/W74x-1) geladen werden. Konfigurationsdateien, die mit einem Gerät der Firmware V3.0 (bzw. 3.2 oder 3.3) erzeugt wurden, können jedoch nicht in Geräte mit dem FW-Stand V2.4 oder älter geladen werden.

Wiederverwendung von Konfigurationsdaten

Das Abspeichern und Einlesen von Konfigurationsdaten reduziert den Aufwand, wenn mehrere Geräts die gleiche Konfiguration erhalten sollen und wenn die Zuweisung der IP-Adressen über DHCP erfolgt. Speichern Sie die Konfigurationsdaten auf einem PC, nachdem Sie einen SCALANCE W-700 konfiguriert haben. Laden Sie diese Datei auf alle weiteren Geräte, die Sie konfigurieren wollen. Gegebenenfalls müssen Sie diesen Geräten vorher mit dem Primary Setup Tool eine IP-Adresse zuweisen.

So laden bzw. speichern Sie Daten über HTTPS

1. Geben Sie für die Konfigurationsdaten bzw. die Firmware im entsprechenden Eingabefeld den Namen der Datei an, aus der Daten übernommen bzw. in der Daten gespeichert werden sollen.
   Alternativ dazu können Sie auch einen Dateiauswahl-Dialog nutzen, der sich nach Anklicken der Schaltfläche "Durchsuchen..." öffnet.
2. Starten Sie das Speichern durch Anklicken der Schaltfläche Save. Das Laden aus der Datei starten Sie durch Anklicken der Schaltfläche "Load".

So laden bzw. speichern Sie Daten über TFTP

1. Geben Sie die IP-Adresse des TFTP-Servers im Eingabefeld TFTP Server IP ein.
2. Geben Sie den Port des TFTP-Servers im Eingabefeld Port ein, falls der Vorgabewert nicht Ihren Anforderungen entspricht.
3. Klicken Sie die Schaltfläche Set Values, bevor Sie weitere Angaben für das Speichern von Daten machen.

4. Geben Sie für die Konfigurationsdaten bzw. die Firmware im entsprechenden Eingabefeld den Namen der Datei an (maximal 32 Zeichen), aus der Daten übernommen bzw. in der Daten gespeichert werden sollen.
5. Starten Sie das Speichern durch Anklicken der Schaltfläche Save. Das Laden aus der Datei starten Sie durch Anklicken der Schaltfläche Load.

Configuration Package

Sind auf einem Client Sicherheitszertifikate für Client und/oder Server installiert, dann bietet der Client beim Sichern der Konfiguration die Möglichkeit an, die Konfigurationsdatei mit den Zertifikaten zusammen als Configuration Package zu speichern. Mittels des Configuration Package können Clients auf einfache Art und Weise repliziert werden, d. h. es werden identische Einstellungen UND Zertifikate in einem Schritt auf die Clients übertragen. Wie beim Laden der Konfigurationsdatei wird im Anschluss ein Neustart ausgeführt. Eine gesonderte Behandlung beim Laden der Konfiguration ist nicht notwendig, der SCALANCE W-700 erkennt selbständig, welchen Typ die Konfigurationsdatei hat.

Siehe auch

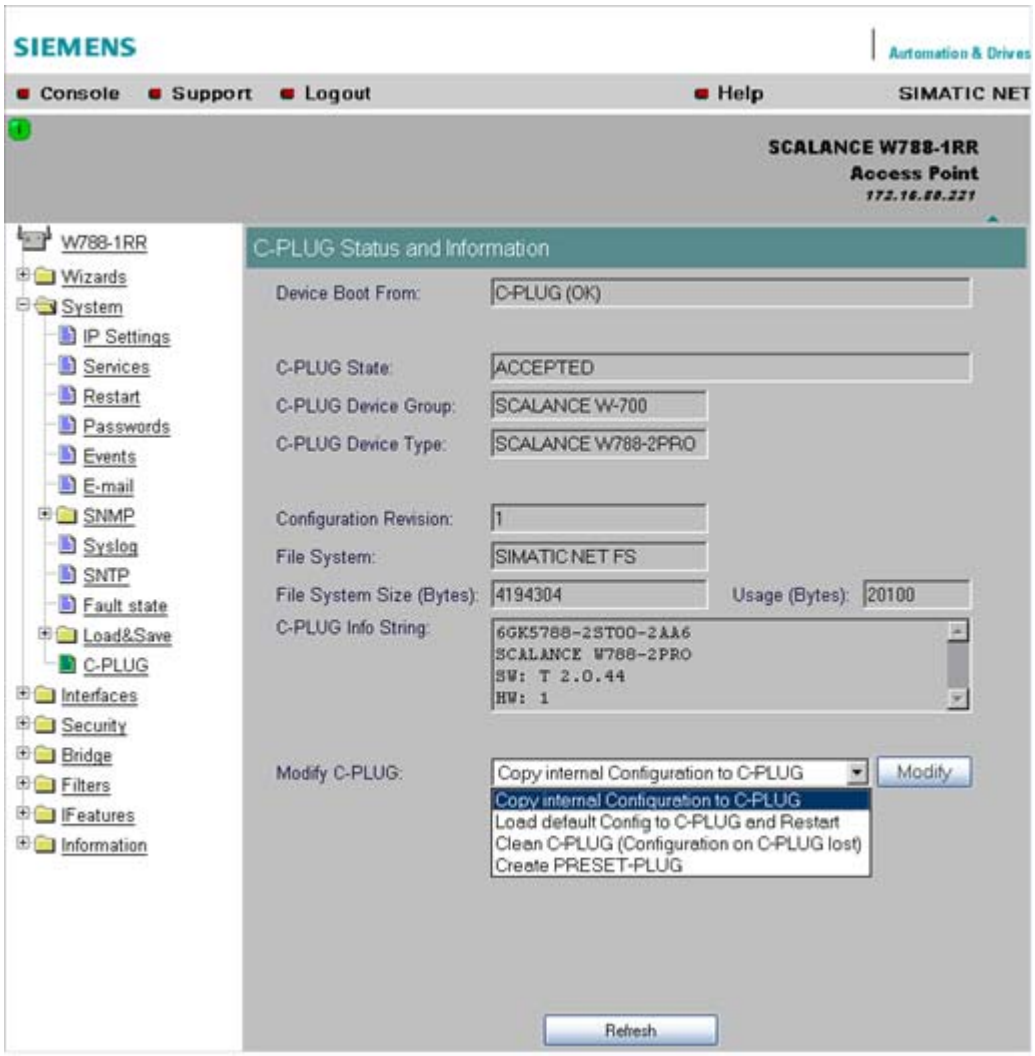
- Menüpunkt CLI\SYSTEM\LOADSAVE (Seite 214)

5.6.3.12 Menüpunkt C-PLUG

Informationen über den Inhalt des Wechselmediums

Dieser Menüpunkt liefert Detailinformationen über den C-PLUG. Darüber hinaus gibt es die Möglichkeit, den C-PLUG zu formatieren oder mit einem neuen Inhalt zu versehen. Sobald das Gerät mit gestecktem C-PLUG gestartet wird, läuft der Scalance W mit den Konfigurationsdaten auf dem C-PLUG an. Die Änderung von Parametern werden auf dem C-PLUG gespeichert und über Web und CLI angezeigt.

Die Daten im Speicher des Gerätes sind erst wieder zugänglich, wenn das Gerät ohne C-PLUG über die Funktion <Restart without C-PLUG> neu anläuft.



Hinweis

Im Bezug auf den C-PLUG arbeiten SCALANCE W-700-Geräte in zwei Modi:

- **Ohne C-PLUG**
  Das Gerät speichert die Konfiguration auf dem internen Speicher. Dieser Modus ist aktiv wenn kein C-PLUG gesteckt ist.
- **Mit C-PLUG**
  Die Konfiguration, die auf dem C-PLUG gespeichert ist, wird über die Benutzerschnittstellen angezeigt. Der interne Speicher wird in diesem Modus weder gelesen noch beschrieben. Bei Änderungen der Konfiguration speichert das Gerät die Konfiguration direkt auf dem C-PLUG. Dieser Modus ist aktiv, sobald ein C-PLUG gesteckt ist. Sobald das Gerät mit gestecktem C-PLUG gestartet wird, läuft der SCALANCE W-700 mit den Konfigurationsdaten auf dem C-PLUG an.

Eingabefeld *C-PLUG State*

Hier wird der Status des C-PLUG angezeigt. Es gibt die folgenden Möglichkeiten:

- ACCEPTED
  Es ist ein C-PLUG mit einem gültigen und passenden Inhalt im Gerät vorhanden.
- NOT ACCEPTED
  Fehlender C-PLUG oder ungültiger bzw. inkompatibler Inhalt eines gesteckten C-PLUG. Dieser Status wird auch angezeigt, wenn der C PLUG im Betrieb formatiert wurde.
- NOT ACCEPTED, HEADER CRC ERROR
  Es ist ein C-PLUG mit fehlerhaftem Inhalt gesteckt.
- NOT PRESENT
  Im Gerät ist kein C-PLUG gesteckt.

Eingabefeld *C-PLUG Device Group*

Gibt an, von welcher SIMATIC NET-Produktlinie der C-PLUG im vorangegangenen Betrieb genutzt wurde.

Eingabefeld C-PLUG Device Type

Gibt den Gerätetyp innerhalb der Produktlinie an, von dem der C-PLUG im vorangegangenen Betrieb genutzt wurde.

Eingabefeld *Configuration Revision*

Die Version der Konfigurations-Struktur. Diese Angabe betrifft die vom Gerät unterstützten Konfigurationsmöglichkeiten und hat nichts mit der konkreten Hardwarekonfiguration zu tun. Diese Revisionsangabe ändert sich also nicht, wenn Sie Module bzw. Extender hinzufügen oder entfernen, sie kann sich aber ändern, wenn Sie einen Firmwareupdate durchführen.

Eingabefeld *File System*

Zeigt den Typ des Dateisystems an, das auf dem C-PLUG vorhanden ist.

Eingabefeld *File System Size*

Zeigt die maximale Speicherkapazität des Dateisystems an, das auf dem C PLUG vorhanden ist.

Eingabefeld *File System Usage*

Zeigt den belegten Speicherplatz im Dateisystem des C-PLUG an.

Eingabefeld *C-PLUG Info String*

Hier werden zusätzliche Informationen über das Gerät angezeigt, das den C PLUG im vorangegangenen Betrieb genutzt hatte, z. B. Bestellnummer, Typenbezeichnung sowie die Ausgabestände von Hardware und Software.

Klappliste Modify C-PLUG, Schaltfläche Modify

Sie können in diesem Feld nur dann Einstellungen vornehmen, wenn Sie als "Admin" eingeloggt sind. Wählen Sie hier aus, wie Sie den Inhalt des C PLUG verändern wollen. Es gibt folgende Alternativen:

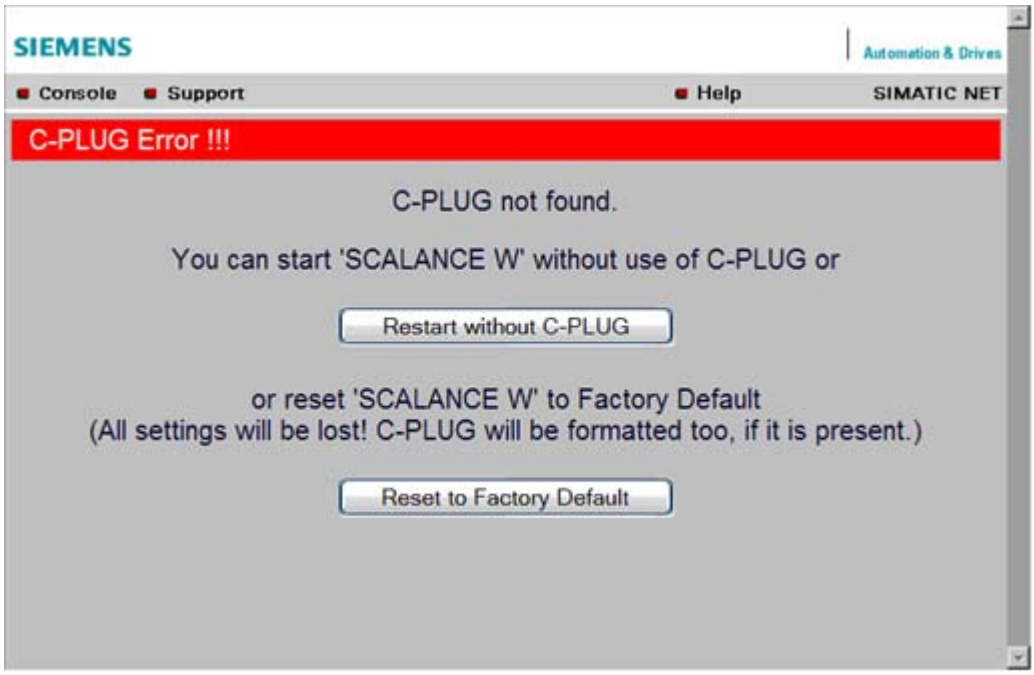
- Copy internal Configuration to C-PLUG
  Die im internen Flash des SCALANCE W-700 vorhandene Konfiguration wird auf den C-PLUG kopiert, anschließend erfolgt ein Neustart.
  Für diese Funktion gibt es folgenden wichtigen Einsatzfall: Das Gerät ist mit einem C-PLUG angelaufen, der eine vom Gerät abweichende oder fehlerhafte Konfiguration enthält. Wenn Sie nach dem Gerätestart noch keine Konfigurationsänderung durchgeführt haben, können Sie mit dieser Funktion den Inhalt des C-PLUG mit der ursprünglichen Gerätekonfiguration aus dem Speicher überschreiben.
- Load default Configuration to C-PLUG and Restart
  Eine Konfiguration mit allen Factory Default-Werten wird auf dem C PLUG gespeichert. Anschließend erfolgt ein Neustart, wobei das Gerät mit diesen Defaultwerten hochläuft.
- Clean C-PLUG (Low Level Format, Configuration lost)
  Löscht alle Daten vom C-PLUG und führt eine Low Level-Formatierung durch. Es erfolgt kein automatischer Neustart.
- Create PRESET-PLUG
  Schreibt Konfigurationsdaten in einen PRESET-PLUG. Ausführliche Informationen zu diesem Thema finden Sie in Kapitel "Konfiguration mit dem PRESET-PLUG".

Nach erfolgter Auswahl starten Sie die Durchführung, indem Sie die Schaltfläche "Modify" anklicken

Meldung bei einem C-PLUG-Fehler

Wenn das Gerät beim Hochlauf einen C-PLUG-Fehler feststellt, wird über das Web Based Management eine entsprechende Meldung ausgegeben. C PLUG-Fehler können zwei Ursachen haben:

- Der C-PLUG enthält fehlerhafte Daten oder Daten für einen anderen Gerätetyp.
- Im Gerät ist kein C-PLUG vorhanden, obwohl vor dem letzten Herunterfahren des Geräts noch ein C-PLUG vorhanden war.



Siehe auch

- Menüpunkt CLI\SYSTEM\CPLUG (Seite 216)

5.6.4 Das Menü Interfaces

5.6.4.1 Menüpunkt Interfaces

Einleitung

Der SCALANCE W-700 hat eine Ethernet-Schnittstelle und eine oder mehrere WLAN-Schnittstellen, die unabhängig voneinander konfiguriert werden können. Mit den Seiten dieses Menüs können Sie sowohl die drahtgebundene Ethernet-Schnittstelle als auch die WLAN-Schnittstelle konfigurieren.

Außerdem können Sie in der Betriebsart Access Point über den Untermenüpunkt Interfaces > WLAN1…3 > Virtual AP count bis zu acht virtuelle Accesspoints (VAP0 … VAP7) pro Wireless-Schnittstelle konfigurieren.

Hinweis

VAPs sind erst nach AP count > 0 sichtbar.

5.6.4.2 Menüpunkt Ethernet

Übertragungsgeschwindigkeit und Betriebsart

Für die drahtgebundene Ethernet-Schnittstelle mit RJ45-Anschluss werden die Parameter Übertragungsgeschwindigkeit / Betriebsart und Kreuzen der Ethernet Verbindung festgelegt. Wenn Sie in der Klappliste "Speed / Mode" den Eintrag Auto auswählen, legt das Gerät abhängig von den anderen Netzteilnehmern Geschwindigkeit / Betriebsart und Kreuzen der Ethernet Verbindung geeignet fest.

Wenn Sie in der Klappliste "Speed / Mode" einen anderen Eintrag als "Auto" auswählen, müssen Sie mittels "Ethernet crossing" das Kreuzen der Ethernet Verbindung manuell festlegen.

Hinweis

Wenn Sie die Betriebsart fest einstellen, müssen Sie beim Partnergerät die gleichen Einstellungen vornehmen.

Für Geräte mit ST-Duplex Multimode Lichtwellenleiter-Anschluss erfolgt keine Parametrierung. Es werden die Ethernet MAC-Adresse und die aktuelle Übertragungsgeschwindigkeit/Betriebsart angezeigt.

Siehe auch

- Menüpunkt CLI\INTERFACES\ETHERNET (Seite 217)

5.6.4.3 Menüpunkt WLAN

Schnittstelle aktivieren

Aktivieren Sie die Schnittstelle, indem Sie "Enable Interface" markieren.

Netzwerkname (Nur im Access Point-Modus)

Geben Sie im Eingabefeld "SSID" den Netzwerknamen des drahtlosen Netzwerks ein. Wenn Sie den Basic Wizard verwendet haben, ist hier bereits ein Wert eingetragen.

Infrastructure / Ad-Hoc (Nur für Clients oder Access Points im Client-Modus)

Wählen Sie Infrastructure aus, um sich mit einem Access Point zu verbinden. "Ad-Hoc" dient dazu, Clients ohne Access Point miteinander zu verbinden. Dazu müssen alle Clients auf "Ad-Hoc" eingestellt sein.

Übertragungsverfahren

Legen Sie in der Klappliste "Wireless Mode" das Übertragungsverfahren fest. Wenn Sie den Basic Wizard verwendet haben, ist hier bereits ein Wert eingetragen.

Hinweis

Übertragungsverfahren IEEE 802.11h

Die Auswahl des Protokolls 802.11h ist nicht in allen Ländereinstellungen möglich. Sie wird durch die Konfiguration von Country code auf der Seite System festgelegt.

Bei Auswahl des Protokolls 802.11h wird nach Übernahme der Konfiguration mit Set Values hinter dem Optionskästchen Enable Interface der Kommentar "(DFS is active for this country code)" angezeigt.

Mit der automatisch aktivierten Funktion Dynamische Frequenzbandwahl (DFS) prüft der Access Point vor Aufnahme der Kommunikation, ob der konfigurierte bzw. gewählte Kanal (siehe Auto Channel Select) frei von Signalen eines Primärnutzers (z.B. Radar) ist.

Werden auf dem gewählten oder konfigurierten Kanal Signale eines Primärnutzers entdeckt, dann geht der Access Point folgendermaßen vor:

- "Auto channel select" = aktiviert
  Bei automatischer Kanalwahl weicht der Access Point auf einen anderen Kanal aus und wiederholt für diesen Kanal die Verfügbarkeitsprüfung.
- "Auto channel select" = deaktiviert
  Bei fest konfiguriertem Kanal weicht der Access Point auf den konfigurierten

Alternativkanal aus und wiederholt für diesen Kanal die Verfügbarkeitsprüfung. Wird auch auf dem Alternativkanal ein Primärnutzer (z.B. Radar) entdeckt, wird ein weiterer zufälliger Kanal gewählt.

Erst wenn der Access Point für eine Minute auf dem gewählten Kanal keinen Primärnutzer findet, wird die Kommunikation mit den Clients aufgenommen.

Beim Betrieb von PNIO-Anlagen mit dem Funkstandard 802.11h ist sicherzustellen, dass keine Radarsignale in der Anlagenumgebung auftreten. Die Erkennung von Radarsignalen hat aufgrund der in 802.11h vorgegebenen DFS-Strategie einen Kanalwechsel zur Folge.

Outdoor AP mode (Nur im Access Point-Modus) / Outdoor Client mode (Nur für Clients oder Access Points im Client-Modus)

Das Gerät kann entweder im Indoor- oder im Outdoor-Modus betrieben werden. Im Indoor-Modus stehen alle länderabhängig zugelassenen Kanäle und Sendeleistungen für den Betrieb in einem Gebäude zur Verfügung. Im Outdoor-Modus ist die Auswahl der länderspezifisch verfügbaren Kanäle und Sendeleistung für den Betrieb im Freien eingeschränkt. Durch Markieren von "Outdoor AP mode" bzw. "Outdoor Client mode" aktivieren Sie diesen Modus.

Kanalauswahl

Bei Clients oder Access Points im Client-Modus können Sie einen Kanal nur im Ad-Hoc-Modus einstellen.

Für Access Points gibt es folgende Möglichkeiten: Markieren Sie das Optionskästchen "Auto Channel Select", wenn sich der Access Point selbst einen freien Kanal suchen soll. Wenn Sie einen Kanal fest vorgeben wollen, darf "Auto Channel Select" nicht markiert sein. Sie können in der Klappliste "Radio Channel" einen geeigneten Kanal festlegen.

Übertragungsverfahren IEEE 802.11h:

Wenn Sie im Access Point-Modus als Übertragungsverfahren das Protokoll 802.11h gewählt haben und "Auto Channel Select" nicht markiert ist, dann wird unter "Radio channel" das Eingabefeld "Alt. radio channel" eingeblendet. Legen Sie dort den Alternativkanal für den Fall fest, dass auf dem Hauptkanal Signale eines Primärnutzers entdeckt wurden.

Stellen Sie sicher, dass der Alternativkanal nicht von anderen Access Points genutzt wird.

Im Übertragungsverfahren IEEE 802.11h ist es nicht sinnvoll, die Betriebsart WDS zu wählen. In der Betriebsart WDS müssen alle Access Points den gleichen Kanal benutzen. Wird jetzt von einem Access Point ein Signal eines Primärnutzers entdeckt, wird der Kanal automatisch gewechselt und dadurch die bestehende Verbindung unterbrochen.

MAC-Adresse des Clients (Nur für Clients oder Access Points im Client-Modus)

Für die an der Ethernet Schnittstelle des Clients angeschlossenen Geräte muss zur Erreichbarkeit eine MAC-Adresse festgelegt werden. Diese MAC-Adresse wird vom Client zur Funkkommunikation mit dem Access Point verwendet. Dies kann automatisch geschehen, indem der Client die MAC-Adresse des ersten Telegramms annimmt, welches er über die Ethernet Schnittstelle empfängt. Dazu muss "Auto find Adopt MAC" ausgewählt werden.

Solange der Client auf ein Ethernet-Frame wartet, meldet er sich beim Access Point mit seiner eigenen MAC-Adresse an. Sobald das erste Ethernet-Frame empfangen wurde, meldet sich der Client beim Access Point ab um sich gleich danach mit der MAC-Adresse aus dem Ethernet-Frame wieder anzumelden. Erfolgt nun ein Link-Down am Ethernet-Port, meldet sich der Client am Access Point ab und wieder mit seiner eigenen MAC-Adresse an.

Falls mehrere Geräte am Client angeschlossen sind, sollte diese Einstellung nicht gewählt werden.

Weiterhin gibt es noch die Möglichkeit, die MAC-Adresse des angeschlossenen Geräts manuell festzulegen. Dazu markieren Sie "Set 'Adopt MAC' manually" und geben im

Eingabefeld "Adopt MAC" die MAC-Adresse des Gerätes an, welches am Client angeschlossen ist.

Um ein komplettes Netzwerk von Geräten hinter dem Client ansprechen zu können, muss "Adopt own MAC" markiert sein. In diesem Fall sind nur Layer 3 Verbindungen möglich (TCP/IP). Für die Gerätevariante SCALANCE W744-1PRO und SCALANCE W744-1 ist das allerdings nicht möglich.

Falls hinter dem Client bis zu acht MAC-Adressen bedient werden sollen, muss die Einstellung "Layer 2 Tunneling" für den Client gewählt werden.

Hinweis

Die Layer 2 Tunneling- Funktionalität wird von SCALANCE W-700 Access Points ab der Firmware Version V3.1 unterstützt. Diese Einstellung erfüllt Forderungen von Industrie-Applikationen, bei denen MAC-Adressen basierte Kommunikation an mehrere Geräte hinter dem Client benötigt wird. Clients mit dieser Einstellung können sich nicht auf Standard-Wifi-Geräte und SCALANCE W-700 Access Points mit Firmware V3.0 oder älter verbinden.

Virtual AP count (Nur im Access Point-Modus)

Wenn Sie virtuelle Access Points (VAP) an diesem AP konfigurieren wollen, dann legen Sie die Anzahl der virtuellen Access Points über die Klappliste "Virtual AP count" fest. Wenn "Virtual AP count = 0 und VLAN/Prio Tag" deaktiviert sind, werden keine VAPs angelegt.

Sie können max. 8 VAPs definieren. Die Einstellungen von VAP0 werden direkt unter "Interfaces/WLAN" vorgenommen, die Einstellungen für VAP1...7 sind in den Untermenüs "Interfaces/WLAN/VAP1...7" zu finden.

Mit Hilfe von virtuellen Access Points können verschiedene SSIDs (max. 8 pro WLAN Interface) mit unterschiedlichen Security Einstellungen konfiguriert werden. Sie können jeden Virtual AP einem bestimmten VLAN zuordnen.

Set Values

Übernehmen Sie die Konfiguration, indem Sie auf "Set Values" klicken.

Wenn Sie in der Betriebsart "Access Point" virtuelle Access Points konfiguriert haben ("Virtual AP count > 0"), dann werden Sie nach Klick auf "Set Values" aufgefordert, für den SCALANCE W78x einen Neustart durchführen zu lassen.

5.6.4.4 Menüpunkt Advanced

Konfiguration des Sendeverhaltens

Auf dieser Seite können Sie Details des Sendeverhaltens festlegen. Sie müssen die Parameter dieser Seite nur anpassen, wenn das Gerät mit den Standardeinstellungen nicht in der vorgesehenen Art und Weise genutzt werden kann.

Sendeleistung

In der Klappliste Transmit Power können Sie die Sendeleistung des Geräts festlegen. Die Verminderung der Sendeleistung kann bei der Verwendung von Antennen notwendig werden, um die gesetzlich vorgeschriebene maximale Sendeleistung nicht zu überschreiten. Eine Verminderung der Sendeleistung bewirkt eine gezielte Reduktion der Zellengröße.

Beacons

Beacons sind zyklisch versendete Pakete, mit denen ein Access Point die Clients über seine Existenz informiert. Im Eingabefeld "Beacon Interval" legen Sie das Interval fest, mit der das Gerät Beacons sendet.

Nur im Access Point-Modus
Der Parameter "Data Beacon Rate DTIM" (Delivery Traffic Indication Map), legt fest, wie häufig der Access Point Broadcast- und Multicast-Pakete über die drahtlose Schnittstelle sendet. Wenn Sie in dieses Feld 1 eintragen, überträgt der Access Point Broadcast- und Multicast-Pakete direkt nach jedem Beacon (empfohlene Einstellung für normale Netzwerkumgebungen). Der Wert 5 würde bedeuten, dass der Access Point die Broadcast- und Multicast-Pakete sammelt und nach jedem fünften Beacon sendet.

Ein Vergrößern dieses Werts erlaubt den verbundenen Clients einen längeren Sleep-Modus auf Kosten einer höheren Verzögerung bei Broadcast- und Multicast-Paketen.

Hinweis

Als "Beacon Rate" wird die kleinste eingestellte Basic Rate im Menü INTERFACE\WLAN\DATARATES genutzt. Je höher die Datenrate des Beacons eingestellt ist, desto geringer ist die Reichweite des Beacons.

RTS/CTS

RTS/CTS (Request To Send/Clear To Send) ist ein Verfahren zur Kollisionsvermeidung, das auf dem Austausch von Statusinformationen vor dem Senden der eigentlichen Daten beruht (Hidden node problem). Um die Netzbelastung durch den zusätzlichen Protokollverkehr zu minimieren, wird dieses Verfahren erst ab einer Paketgröße angewendet, die Sie mit dem Parameter "RTS/CTS Threshold" festlegen.

Fragmentierung

Mit dem Parameter "Fragmentation Length Threshold" wird die maximale Paketgröße festgelegt, die auf der Funkstrecke übertragen wird. Größere Pakete werden vor dem Senden in kleinere aufgeteilt und nach dem Empfangen wieder zur ursprünglichen Größe zusammengesetzt. Dies kann bei sehr schlechter Übertragungsqualität vorteilhaft sein, da größere Pakete schwieriger zu übertragen sind. Jedoch bringt die Fragmentierung in kleinere Pakete einen schlechteren Datendurchsatz mit sich.

Wiederholungen

Es gibt zwei Instanzen, bei denen Pakete wiederholt werden. Die Hardware-Wiederholung wird vom WLAN Chip selbst durchgeführt, indem er versucht, ein nicht quittiertes Paket sofort zu wiederholen. Die Anzahl dieser Versuche wird mit dem Parameter "HW Retry number" festgelegt.

Waren alle Hardware-Wiederholungen erfolglos, wird das Paket zurückgestellt und zuerst alle anderen im Buffer befindlichen Pakete gesendet. Danach wird erneut versucht, das Paket zu versenden. Die Anzahl solcher Wiederholungen wird mit dem Parameter "SW Retry number" festgelegt.

Mittels "Use SW Retry" kann der Wiederholungsmechanismus der Software ein- oder ausgeschaltet werden.

Verkürzte Präambel beim Verfahren 802.11b

Der Standard 802.11b erlaubt die Verwendung verkürzter Präambeln bei der drahtlosen Übertragung von Datenpaketen. Dadurch wird der Umfang der Nutzdaten erhöht.

Antenna Gain

Der Parameter "Antenna Gain" beschreibt den Antennen-Gewinn in dBi einer am SCALANCE W-700 angeschlossenen Antenne.

Sie können für folgende Parameter Werte festlegen:

- "Antenna Type"
- "Antenna Gain"
- "Antenna cable length (in meters)"

Steht "Antenna Type" auf "User Defined", können Sie in das Feld "Antenna Gain" einen beliebigen Wert für den Antennengewinn eintragen. Andernfalls wird der vorkonfigurierte Wert des gewählten "Antenna Type" angezeigt. Im Feld "Antenna cable length (in meters)" geben Sie die Länge des Verbindungskabels zwischen Gerät und Antenne an.

Die Angabe spezifischer Werte ist notwendig, um sicherzustellen, dass die jeweiligen länderspezifischen Bestimmungen der Regulierungsbehörden eingehalten werden. Durch die Regulierungsbehörden werden zum Beispiel alle nutzbaren Kanäle, die zugehörige maximale Sendeleistung und weitere Nutzungsbedingungen festgelegt. Weitere Details zu den Bestimmungen Ihres Landes können über countrylist.log eingesehen werden.

Der SCALANCE W-700 bestimmt aus den Angaben zum Antennengewinn und zur Sendeleistung selbständig die zulässigen Kanäle. Für Antennen mit hohem Antennengewinn stehen unter Umständen weniger zulässige Kanäle zur Verfügung als für Antennen mit geringem Antennengewinn.

Hinweis

Mit der Auswahl des Wertes "User defined" wird Ihnen die Möglichkeit gegeben, ganzzahlige dBi-Werte für den Antennengewinn im Bereich von 0 - 30 dBi einzutragen. Bitte berücksichtigen Sie auch die Verluste des Antennen-Anschlusskabels.

ACHTUNG
Die richtige Antenneneinstellung ist für einen zulassungskonformen Betrieb unbedingt notwendig. Ein falscher Eintrag des Antennengewinns kann strafrechtlich geahndet werden!

Antennen

Die Klappliste "Antenna Mode" legt die Verwendung der Antennen fest.

- Die Einstellung Diversity nimmt zur Datenübertragung die bestmögliche der beiden Antennen. Dazu müssen pro WLAN-Schnittstelle beide Antennen angeschlossen sein. Des Weiteren sollten beide Antennen vom gleichen Typ sein und beide Antennen sollten ungefähr den gleichen Raum ausleuchten. Wenn ein Access Point mit Diversity-Einstellung betrieben wird und die beiden Antennen verschiedene Funkzellen aufspannen, kann dies negative Effekte hervorrufen.
- In der Einstellung "Tx on A, Rx on B" wird Antenne A zum Senden und Antenne B zum Empfangen benutzt.
- In der Einstellung "Tx on B, Rx on A" wird Antenne B zum Senden und Antenne A zum Empfangen benutzt.

In den Einstellungen "Diversity, Tx on A, Rx on B" sowie "Tx on B, Rx on A" müssen pro WLAN Schnittstelle zwingend beide Antennen angeschlossen sein. Ist nur eine Antenne angeschlossen, dann muss die angeschlossene Antenne fest eingestellt werden. Zusätzlich muss die zweite Antennenbuchse mit einem 50 Ω-Abschlusswiderstand versehen werden.

Hinweis

Informationen über die Lage der Antennenbuchsen finden Sie im Kapitel "Anschlüsse für externe Antennen".

Suche nach Access Points (Nur bei Clients und Access Points im Client-Modus)

Während der Client mit einem Access Point verbunden ist, sucht er im Hintergrund nach weiteren Access Points, mit denen er sich gegebenenfalls verbinden kann. Für das Suchen nach weiteren Access Points gibt es drei Modi, die über die Klappliste "Background scan mode" eingestellt werden können.
Bei "Disable" wird nie nach weiteren Access Points gesucht, solange der Client verbunden ist.
Bei "Scan if Idle" wird erst nach weiteren Access Points gesucht, wenn für eine bestimmte Zeit kein Datentransfer stattfindet.
Bei "Scan Always" wird kontinuierlich nach weiteren Access Points gesucht.
Der Parameter "Background scan interval" legt das Intervall fest, in dem nach weiteren Access Points gesucht wird.

Um die Suche nach anderen Access Points zeitlich zu optimieren, kann man dem Client die Kanäle vorgeben, auf denen andere Access Points zu finden sind. Dazu muss das Opionskästchen "Background Scan Ch.Select" gesetzt und im Eingabefeld "Background Scan Channels" die Kanäle der anderen Access Points eingetragen werden. Die Kanäle sind durch Leerzeichen getrennt einzutragen.

Hat der Client einen besseren Access Point gefunden, versucht er sich mit diesem zu verbinden. Dazu muss der neue Access Point um einen bestimmten Wert besser sein als der aktuelle. Die Schwelle, ab wann der Client zum neuen Access Point wechselt, kann mit dem Parameter "Roaming threshold" festgelegt werden.

Roaming bei fehlender Ethernet-Schnittstelle (Nur im Access Point-Modus)

Wenn die drahtgebundene Ethernet-Schnittstelle nicht mehr zur Verfügung steht (Kabelbruch, Stecker gezogen), erhält ein über das Funknetz angebundener Client davon keine Kenntnis. Der Access Point kann dann die angemeldeten WLAN-Clients zu einem Roaming zwingen, indem er sein WLAN-Interface deaktiviert. Der Client wird dann versuchen, sich bei einem anderen Access Point anzumelden. Sie aktivieren diese Eigenschaft, indem Sie das Optionskästchen "Force roaming if link down on the ethernet interface" markieren.

Enable WMM

Mit Wireless Multimedia werden Multimedia-Telegramme gemäß dem Standard IEEE 802.11e mit einer höheren Priorität übertragen.

Markieren Sie die Option Enable WMM, wenn Telegramme nach ihrer Priorität bewertet und priorisiert über die WLAN-Schnittstelle gesendet werden sollen.

Nach dem Wi-Fi-Standard werden priorisierte Telegramme folgendermaßen für WMM klassifiziert:

Access Category	Description	802.1d Tags
WMM voice priority	Highest priority Allows multiple concurrent VoIP calls, with low latency and toll voice quality	7, 6
WMM Video priority	Prioritize video traffic above other data traffic. One 802.11g or 802.11a channel can support 3-4 SDTV streams or 1 HDTV streams.	5, 4

Access Category	Description	802.1d Tags
WMM best effort priority	Traffic from legacy devices, or traffic from applications or devices that lack QoS capabilities. Traffic less sensitive to latency, but affected by long delays, such as Internet surfing.	0, 3
WMM background priority	Low priority traffic (file downloads, print jobs) that does not have strict latency and throughput requirements.	2, 1

5.6.4.5 Menüpunkt SSID List

Hinweis

Der Untermenüpunkt "SSID List" ist nur für Clients und Access Points im Client-Modus verfügbar. Die Betriebsart können Sie im Menü "System" festlegen.

Netzanbindung für den Client

In diesem Menüpunkt können Sie festlegen, wie sich das Gerät als Client mit einem Netz verbindet:

- Ist das Optionskästchen Connect to ANY SSID markiert, versucht sich das Gerät im Client-Modus mit dem Netzwerk zu verbinden, das die beste Übertragungsqualität besitzt und über passende Security-Einstellungen verfügt. Wenn für einen Access Point die Einstellung "Suppress SSID broadcasting" gilt, kann sich der Client dort nicht mit der SSID ANY anmelden.
- Ist dieses Optionskästchen nicht markiert, versucht der Client sich mit dem Netzwerk aus der SSID Liste zu verbinden, das die beste Übertragungsqualität bietet.

Bei Ad-Hoc-Netzwerken und iPCF wird eine SSID unbedingt benötigt. Die maximale Anzahl der SSID´s in der SSID Liste ist auf 32 begrenzt.

Siehe auch

- Menüpunkt CLI\INTERFACES\WLAN1\SSID (bzw. \WLAN2\SSID oder \WLAN3\SSID) (Seite 223)

5.6.4.6 Menüpunkt Advanced G

Eigenschaften des 802.11g-Standards

Der Standard IEEE 802.11g ist abwärtskompatibel zu IEEE 802.11b, beide nutzen das 2,4 GHz-Band. Im Gegensatz zum Funkmodus 802.11b, der Datenraten bis 11 Mbit/s spezifiziert, bietet 802.11g Übertragungsraten bis 54 Mbit/s. Darüber hinaus benutzt der 802.11g-Standard das Modulationsverfahren OFDM. Diese Technologie teilt ein Datenpaket in mehrere kleinere Pakete auf, die gleichzeitig mit unterschiedlichen Frequenzen übertragen werden.

Besondere Einstellmöglichkeiten für 802.11g

Die Einstellmöglichkeiten im Untermenüpunkt "Advanced G" betreffen die Art und Weise, wie Management- und Kontrolldaten (RTS/CTS-Telegramme, Beacons) im 802.11g-Modus versendet werden. Außerdem können Sie festlegen, dass der SCALANCE W-700 nur 802.11g-kompatible Geräte unterstützt.

Behandlung von 802.11b Clients

Der Access Point erkennt automatisch, ob 802.11b Clients in der Umgebung vorhanden sind. Damit 802.11g Pakete nicht mit 802.11b Paketen kollidieren, kann der Access Point das RTS/CTS Verfahren verwenden.

Verwendung von RTS/CTS (Nur im Access Point-Modus)

Mit der Klappliste "802.11g CTS mode" wird die Verwendung von RTS/CTS festgelegt:

None	Kein RTS/CTS verwenden.
Always	Immer RTS/CTS verwenden bei 802.11g Paketen.
Auto	Nur RTS/CTS verwenden, wenn 802.11b Clients in der Umgebung sind.

Die Datenrate für die RTS/CTS Frames kann man über die Klappliste "802.11g CTS Rate" einstellen.

Mit der Klappliste "802.11g CTS Type" legt man fest, ob nur ein CTS oder RTS/CTS gesendet werden soll.

802.11g Erweiterungen

Mit dem Parameter "802.11g Short Slot Time" legt man fest, ob die kurze Slot Time verwendet werden soll. Diese kurze Slot Time sollte von allen neueren Clients unterstützt werden.

Mit dem Parameter "802.11g Only mode" kann man dafür sorgen, dass sich nur 802.11g-Clients am Access Point anmelden können, und auch nur 802.11g-Rates zugelassen sind (nur im Access Point-Modus). In dieser Betriebsart wird ausschließlich das Modulationsverfahren OFDM verwendet. Dadurch wird verhindert, dass sich 802.11b-Geräte anmelden. Wenn der 802.11g Only mode deaktiviert ist, können sich sowohl 802.11b-Geräte als auch 802.11.g-Geräte am Access Point anmelden.

5.6.4.7 Menüpunkt Data Rates

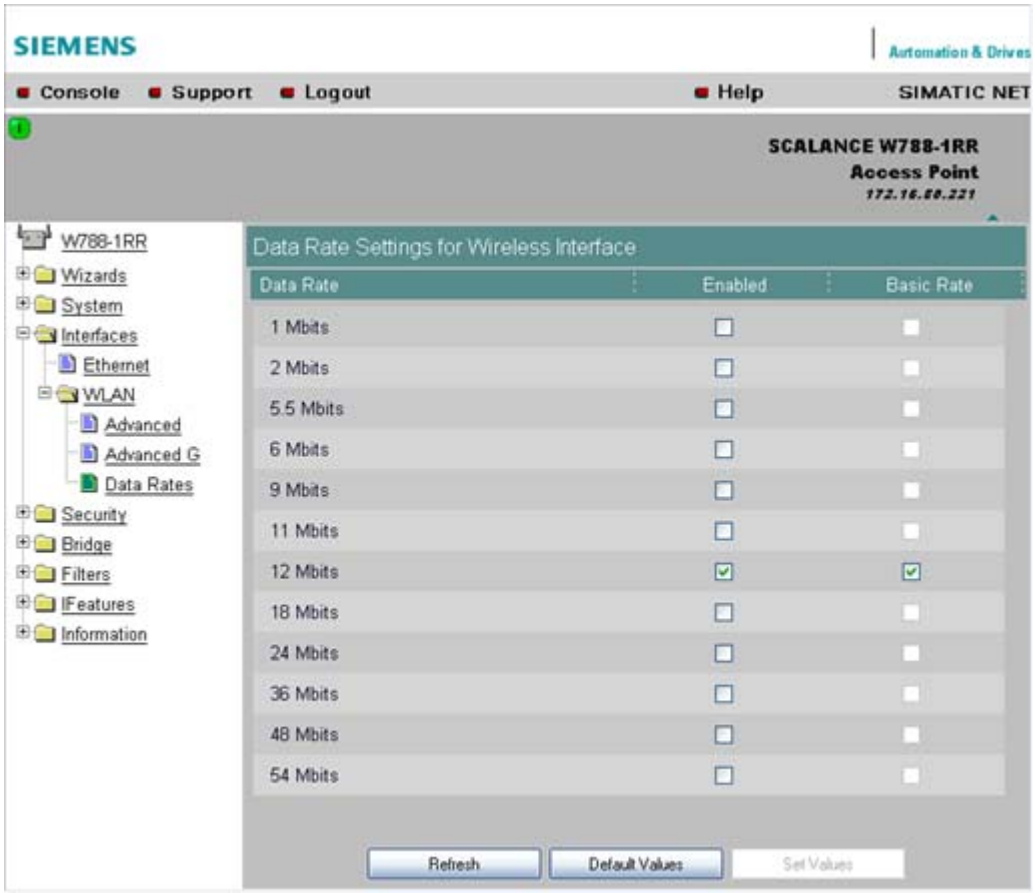
Hinweis

Der Untermenüpunkt "Data Rates" ist nur für im Access Point-Modus verfügbar.

Variable Einstellung der Übertragungsraten

Über eine tabellarische Ansicht, die alle verfügbaren Datenraten für den aktuellen WLAN-Modus (802.11b, g, a usw.) anzeigt, könne Sie eine beliebige Kombination dieser Raten auswählen. Ausschließlich die gewählten Übertragungsraten werden dann vom Access Point zur Kommunikation mit den Clients verwendet.

Der Parameter "Basic Rate" legt fest, dass ein Client die entsprechende Datenrate zwingend beherrschen muss, um sich mit dem Access Point verbinden zu können.



Siehe auch

- Menüpunkt CLI\INTERFACES\WLAN1\DATARATES (bzw. \WLAN2\DATARATES oder \WLAN3\DATARATES) (Seite 225)

5.6.4.8 Menüpunkt VAP

Hinweis

Der Untermenüpunkt "VAP" ist nur im Access Point-Modus verfügbar.

Beschreibung

Die Seiten der virtuellen Access Points VAP1...VAP7 können Sie nur ausfüllen, wenn Sie auf der übergeordneten Ebene "Interfaces > WLAN" virtuelle Access Points konfiguriert haben ("Virtual AP count > 0").

Auf dieser Seite können Sie den virtuellen Access Points eine eigene SSID vergeben, d.h. der Access Point läuft im Multi-SSID-Betrieb.

SSID

Geben Sie hier die SSID des VLAN ein.

Beachten Sie, dass Sie die SSID dieses VLAN auch in der Konfiguration des Client, den Sie diesem VLAN zuordnen, hinterlegen.

Hinweis

Für jeden virtuellen Access Point können Sie separate Sicherheitseinstellungen konfigurieren (siehe Kapitel "Menüpunkt Basic Wireless")

Die Sicherheitseinstellungen der VAPs müssen denen der betreffenden VLANs entsprechen.

Siehe auch

- Menüpunkt CLI\INTERFACES\WLAN1\VAP1..7 (bzw. \WLAN2\VAP1..7 oder \WLAN3\VAP1..7) (Seite 226)

5.6.5 Das Menü Security

5.6.5.1 Menüpunkt Security

Einleitung

In diesem Menü konfigurieren Sie die Sicherheitseinstellungen, mit denen Sie Ihr Gerät betreiben wollen. Dazu gehört neben der Auswahl des Authentifizierungsverfahrens und der Verschlüsselungsmethode auch die Festlegung, ob ein externer Radius-Server genutzt wird und ob eine Zugriffseinschränkung auf Basis der MAC-Adressen (ACL) erfolgt.

Siehe auch

- Menüpunkt CLI\SECURITY (Seite 227)

5.6.5.2 Menüpunkt Basic Wireless

Authentifizierung

Unter Authentifizierung versteht man ganz allgemein das Erbringen eines Identitätsnachweises. Somit schützt die Authentifizierung das Netzwerk vor ungewollten Zugriffen. Im Feld "Security Level" kann zwischen folgenden Authentifizierungsarten gewählt werden:

- **Open System**
  Es wird keine Authentifizierung vorgenommen. Eine Verschlüsselung mit einem festen (nicht wechselnden) Schlüssel kann optional ausgewählt werden. Hierfür müssen Sie im Menü "Keys" einen Schlüssel definieren. 5 bzw. 13 ASCII- oder 10 bzw. 26 hexadezimale Zeichen legen einen schwächeren Schlüssel (40/104 Bit) fest. 16 ASCII- oder 32 hexadezimale Zeichen definieren dagegen einen starken Schlüssel (128 Bit). Danach müssen Sie im Menü "Basic WLAN" den Punkt "Encryption" aktivieren.

  Hinweis

  Bei folgenden Geräten im iPCF-Modus ist nur diese Einstellung möglich:
  - SCALANCE W788-xRR im Client Modus
  - SCALANCE W784-xRR im Client Modus
  - SCALANCE W747-1
  - SCALANCE W747-1RR
  - IWLAN/PB-Link PNIO

- **Shared Key**
  Bei der Shared Key Authentifizierung wird im Client und Access Point ein fester Schlüssel hinterlegt. Dieser wird dann zur Authentifizierung und Verschlüsselung verwendet. Sie müssen in diesem Fall einen WEP-Schlüssel, nach der Wahl von "Low (Shared Key)", hinterlegen.

Hinweis

Nur im Access Point-Modus:

Bei Verwendung von Open System with Encryption bzw. Shared Key in Verbindung mit ACL-Listen sind die Hinweise im Kapitel "Menüpunkt ACL" zu beachten.

- **WPA2-PSK**
  WPA2-PSK basiert auf dem Standard WPA2, die WPA-Authentifizierung arbeitet jedoch ohne RADIUS-Server. Statt dessen wird **auf jedem** Client und Access Point ein Schlüssel (Pass phrase) hinterlegt und zur Authentifizierung und weiteren Verschlüsselung verwendet. Als Verschlüsselungsmethode wird AES oder TKIP verwendet, AES stellt die Standardmethode dar.

Hinweis

Der Schlüssel kann 8 bis 63 ASCII-Zeichen oder genau 64 hexadezimale Zeichen lang sein. Er sollte komplex (z. B. aus willkürlichen Zahlen, Buchstaben (groß/klein), wenig Wiederholungen und Sonderzeichen) gewählt werden. Nutzen Sie keine bekannten Namen, Wörter und Begriffe, die erraten werden könnten. Bei Verlust eines Gerätes oder bei bekannt werden des Schlüssels sollte aus Sicherheitsgründen der Schlüssel auf allen Geräten geändert werden.

- **WPA2**
  WPA2 (Wi-Fi Protected Access 2) ist die Weiterentwicklung von WPA und implementiert die Funktionen des Sicherheitsstandards IEEE 802.11i. WPA2 nutzt zusätzlich das Verschlüsselungsprotokoll CCMP, das durch Vor-Authentifizierung schnelles Roaming in mobilen Ad-hoc-Netzen ermöglicht. Ein Client kann sich vorab bei mehreren Access Points anmelden, wodurch die laufende Authentifizierung entfällt.
  Zur Authentifizierung des Clients an einem Access Point wird ein RADIUS-Server genutzt. Der Client meldet sich anhand von einem Zertifikat (EAP-TLS) oder der Kombination aus Benutzername und Passwort (EAP-PEAP bzw. EAP-TTLS / innere Authentifizierungsmethode MSCHAPv2) am RADIUS-Server an. Danach weist sich der RADIUS-Server mittels Zertifikat optional gegenüber dem Client aus. Nach einer erfolgreichen Authentifizierung generieren Client und RADIUS-Server Schlüsselmaterial, das für die Datenverschlüsselung verwendet wird. Als Verschlüsselungsmethode wird AES oder TKIP verwendet, AES stellt die Standardmethode dar.
- **WPA-Auto-PSK**
  Einstellung, in der ein Access Point sowohl die Authentifizierungsart "WPA-PSK" als auch "WPA2-PSK" verarbeiten kann. Dies ist erforderlich, wenn der Access Point mit verschiedenen Clients kommuniziert, die einerseits "WPA-PSK" und andererseits "WPA2-PSK" verwenden. Bei den Clients muss das gleiche Verschlüsselungsverfahren eingesetzt werden.
- **WPA-Auto**
  Einstellung, in der ein Access Point sowohl die Authentifizierungsart "WPA" als auch "WPA2" verarbeiten kann. Dies ist erforderlich, wenn der Access Point mit verschiedenen Clients kommuniziert, die einerseits "WPA" und andererseits "WPA2" verwenden. Bei den Clients muss das gleiche Verschlüsselungsverfahren eingesetzt werden.

Verschlüsselung

Die Verschlüsselung schützt die übertragenen Daten vor Abhören und Fälschen. Sie können die Verschlüsselung nur abschalten, wenn Sie bei der Authentifizierung "Open System" gewählt haben. Alle anderen Sicherungsverfahren beinhalten sowohl Authentifizierung als auch Verschlüsselung.

Verschlüsselungsmethoden

Wenn Sie bei der Authentifizierung Open System inkl. Verschlüsselung oder "Shared Key" gewählt haben, müssen Sie im Menü "Keys" einen Schlüssel definieren (s. Kap. "Menüpunkt Keys").

- WEP (Wired Equivalent Privacy)
  Ein schwaches symmetrisches Stromverschlüsselungsverfahren mit lediglich 40 bzw. 104 Bit langen Schlüsseln, basieren auf dem RC4-Algorithmus (Ron’s Code 4).

  Wenn Sie bei der Authentifizierung WPA-PSK oder WPA (RADIUS) gewählt haben, stehen im Feld "Cipher" folgende Alternativen zur Auswahl:

- TKIP (Temporal Key Integrity Protocol)
  Ein symmetrisches Stromverschlüsselungsverfahren mit dem RC4-Algorithmus (Ron’s Code 4). TKIP verwendet im Gegensatz zur schwachen WEP-Verschlüsselung wechselnde Schlüssel, die von einem Hauptschlüssel abgeleitet werden. TKIP kann außerdem gefälschte Pakete erkennen.

- AES (Advanced Encryption Standard)
  Starkes symmetrisches Blockverschlüsselungsverfahren nach dem Rijndael-Algorithmus, der die Funktionen von TKIP weiter verbessert.

- AUTO
  Je nach Fähigkeit der Gegenstation wird entweder AES oder TKIP automatisch ausgewählt.

RADIUS-Authentication Method (Nur für Clients und Access Points im Client-Modus)

Läuft die Authentifizierung eines Client über einen externen RADIUS-Server, kann mit der Hilfe der Auswahlliste "RADIUS authentication type" eine Methode für die äußere Authentifizierung festgelegt werden. Standardmäßig ist der Wert "Auto" ausgewählt, so dass der Client einem RADIUS Server alle unterstützten Methoden anbietet. Jede andere Auswahl schränkt die Unterstützung durch den Client auf diese eine Methode ein. Dieser Schritt kann notwendig sein, da nicht alle RADIUS-Server die Antwort des Client vollständig und korrekt auswerten.

Folgende weitere Auswahlpunkte stehen zur Verfügung:

- EAP TLS - Extensible Authentication Protocol - Transport Layer Security. Nutzt Zertifikate zur Authentifizierung
- EAP TTLS - Extensible Authentication Protocol - Tunnel Transport Layer Security. Nach Aufbau des TLS Tunnels wird MS-CHAPv2 zur inneren Authentifizierung genutzt.
- PEAP - Protected Extensible Authentication Protocol. Alternativer Protokollentwurf der IETF zu EAP-TTLS

Zusätzliche Eingaben für WPA-PSK und WPA2-PSK

Für das Verfahren WPA-PSK müssen Sie im Feld "Pass Phrase" eine Zeichenkette eingeben, die der SCALANCE W74x für die Initialisierung der dynamischen Schlüsselgenerierung verwendet.

Suppress SSID broadcasting (Nur im Access Point-Modus)

Bei der Einstellung Suppress SSID broadcasting ist der SCALANCE W78x grundsätzlich nur für solche Clients zugänglich, die seine SSID kennen. Dieses Verfahren kann verwendet werden, um den SCALANCE W78x vor unberechtigten Zugriffen zu schützen.

Hinweis

Da bei der SSID-Übertragung keine Verschlüsselung eingesetzt wird, kann diese Funktion nur grundlegend vor unberechtigten Zugriffen schützen. Die Nutzung einer Authentifizierungsmethode (z.B. WPA (RADIUS), wenn nicht möglich WPA-PSK) bietet eine höhere Sicherheit.

Es muß zudem damit gerechnet werden, dass bestimmte Endgeräte Probleme mit dem Zugriff auf eine versteckte SSID haben können.

Optionskästchen Inter SSID communication (Nur im Access Point-Modus)

Das Markieren dieses Optionskästchens erlaubt die Kommunikation zwischen WLAN-Clients, die an unterschiedlichen SSIDs eines Accesspoint angemeldet sind.

Beispiel 1:	Ein SCALANCE W78x-2xx oder W786-3PRO wurde mit unterschiedliche SSIDs definiert.
Beispiel 2:	Ein SCALANCE W78x-1xx wird mit Multi-SSIDs verwendet.

Hinweis

Bei einem SCALANCE W78x-2xx oder W786-3PRO muss auf allen WLAN-Schnittstellen beziehungsweise auf allen VAPs die Funktion Inter SSID communication aktiviert werden, um eine Kommunikation zwischen den Clients mit unterschiedlichen SSIDs zu ermöglichen.

Hinweis

Wenn VLANs für die SSIDs konfiguriert sind, kann diese Einstellung die Kommunikation zwischen den SSIDs entsprechend den VLAN-Regeln verhindern.

Klappliste Intracell communication (Nur im Access Point-Modus)

- Intracell blocking
  Diese Einstellung unterbindet die Kommunikation von WLAN-Clients innerhalb einer SSID.
- Ethernet blocking
  Diese Einstellung unterbindet die Kommunikation von WLAN-Clients über die Ethernet-Schnittstelle des Accesspoint.
- Allowed
  Diese Einstellung ermöglicht sowohl die Kommunikation von WLAN-Clients innerhalb einer SSID als auch die Kommunikation von WLAN-Clients über die Ethernet-Schnittstelle.

Übersicht der Kommunikationsmöglichkeiten (Nur im Access Point-Modus)

Zur Verdeutlichung finden Sie hier eine Übersicht, welche Auswirkung die beiden Einstellungen "Inter SSID communication" und "Intracell communication" haben.

Einstellungen		**Mögliche Kommunikation**		
Inter SSID communication	**Intracell communication**	**innerhalb einer SSID**	**zu einer anderen SSID**	**zum Ethernet-Netzwerk**
Enabled	Allowed	X	X	X
Enabled	Intracell blocking		X	X
Enabled	Ethernet blocking	X	X	
Disabled	Allowed	X		X
Disabled	Intracell blocking			X
Disabled	Ethernet blocking	X		

VAP (Nur im Access Point-Modus)

Für jeden der virtuellen Accesspoint VAP1 bis VAP7 konfigurieren Sie hier die folgenden, bereits oben beschriebenen, Sicherheitseinstellungen:

- Authentifizierung
- Verschlüsselung aktivieren
- Verschlüsselungsmethode
- Auswahl des Default-WEP-Schlüssels
- Eingabe des WPA-PSK-Passworts
- Festlegung des "Group Key Update Intervals" bei WPA-PSK
- Aktivierung von "Suppress SSID broadcasting"

Alle anderen Sicherheits-Parameter werden, soweit zutreffend, von der Seite **Security > Basic > WLAN1** bzw. **WLAN2** oder **WLAN3** übernommen.

5.6.5.3 Menüpunkt Keys

Festlegung des WEP-Schlüssels

Damit Sie bei den Authentifizierungsmethoden Open System und Shared Key die Verschlüsselung aktivieren können, müssen Sie zuerst mindestens einen Schlüssel in der Schlüsseltabelle eintragen haben. Hierbei kann zwischen Schlüssellängen gewählt werden. 5 bzw. 13 ASCII- oder 10 bzw. 26 hexadezimale Zeichen legen einen schwächeren Schlüssel (40/104 Bit) fest. 16 ASCII- oder 32 hexadezimale Zeichen definieren dagegen einen starken Schlüssel (128 Bit).

Des Weiteren können für WDS, Redundance und ACL Private Schlüssel angelegt werden (für ACL werden diese nicht von allen Clients unterstützt).

Hinweis

Für Schlüssel können Sie Zeichen mit dem ASCII-Code 0x20 bis 0x7e verwenden. Hier alle unterstützten Zeichen, beginnend mit einem Leerzeichen:

```
 !"#$%&'()*+,-./0123456789:;<=>?@
ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`
abcdefghijklmnopqrstuvwxyz{|}~
```

Siehe auch

- Menüpunkt CLI\SECURITY\KEYS\WLAN1 (bzw. \WLAN2 oder \WLAN3) (Seite 231)

5.6.5.4 Menüpunkt ACL

Hinweis

Das Menü "ACL" ist nur im Access Point-Modus verfügbar.

Zugriffsrechte für einzelne Clients

Die Access Control List (ACL) ist eine Zuordnung von MAC-Adressen und Zugriffsrechten.

Falls die ACL aktiviert ist, überprüft der Access Point vor einem Datentransfer, ob für den Kommunikationspartner (identifiziert durch die MAC-Adresse) die notwendigen Rechte in der ACL-Tabelle eingetragen sind.

Hinweis

Da bei der MAC-Adressen-Übertragung keine Verschlüsselung eingesetzt wird, kann diese Funktion nur grundlegend vor unberechtigten Zugriffen schützen. Die Nutzung einer Authentifizierungsmethode (z.B. WPA (RADIUS), wenn nicht möglich WPA-PSK) bietet eine höhere Sicherheit.

Aktivieren der ACL

Im Web Based Management gibt es eine Klappliste für Verwendung der ACL.

Um die ACL zu aktivieren, müssen Sie die globale Freigabe entweder auf "Enabled" oder auf "Strict" einstellen:

- Enabled
  Alle Clients, die in der ACL eingetragen sind, werden entsprechend dem ACL Eintrag behandelt. Clients die nicht in der ACL eingetragen sind, erhalten Zugriff auf den Access Point. Diese Einstellung kann verwendet werden, um gezielt bestimmten Clients den Zugriff zu verweigern.
- Strict
  Alle Clients, die in der ACL eingetragen sind, werden entsprechend dem ACL Eintrag behandelt. Clients die nicht in der ACL eingetragen sind, erhalten keinen Zugriff auf den Access Point. Diese Einstellung kann verwendet werden, um gezielt bestimmten Clients den Zugriff zu erlauben.
- Disabled
  Die Access Control List wird nicht verwendet.

Eintrag in der ACL ändern

Klicken Sie auf die entsprechende MAC-Adresse, um einen Eintrag in der ACL zu ändern. Mit dem Optionskästchen "Sel" legen Sie fest, ob ein ACL Eintrag verwendet werden soll oder nicht. Das Optionskästchen "Del" dient dazu, einen Eintrag aus der ACL zu löschen.

Neuer Eintrag in der ACL

Klicken Sie die Schaltfläche New, um einen neuen Eintrag in der ACL anzulegen. Es erscheint eine Seite, auf der Sie die notwendigen Festlegungen treffen können. Tragen Sie im Eingabefeld "MAC Address" die MAC-Adresse des Clients ein. Mit der Klappliste "Permission" legen Sie die Zugriffsrechte des Clients fest:

- Allow
  Der Client erhält Zugriff auf den Access Point.
- Deny
  Der Client erhält keinen Zugriff auf den Access Point.
- Default Key
  Der Client erhält nur dann Zugriff auf den Access Point, wenn er den Default Key zur Verschlüsselung der Daten verwendet. Dazu müssen Sie für den SCALANCE W78x (beispielsweise im WBM-Menü "Security") einen gültigen Default Key festlegen, der auch vom Client verwendet wird.
- Private Key
  Mit dieser Einstellung können Sie für verschiedene Clients abweichende Schlüssel verwenden. Die privaten Schlüssel müssen Sie zuvor im Menüpunkt "Keys" anlegen. Mit der Klappliste "Key number" können Sie einen dieser Schlüssel auswählen. Der Client erhält nur dann Zugriff auf den Access Point, wenn er diesen privaten Schlüssel verwendet. Für diese Funktion ist es notwendig, dass der Client private Schüssel unterstützt.

Hinweis

Der in der ACL eingestellte private Schlüssel muss auch auf dem Client in der Schlüsselliste verfügbar sein. Weiterhin muss der Client diesen privaten Schlüssel für die Kommunikation unter Security->Basic->WLAN verwenden (eingestellt haben), sofern Open System with Encryption bzw. Shared Key verwendet werden.

Der private Schlüssel wird bei dieser Verbindung für die übertragenen Unicast-Pakete, welche für den wireless Client bestimmt sind, verwendet.

Alle Multicast- und Broadcast-Pakete werden mit dem auf dem Access Point eingestellten public key übertragen. Daher muss der in der ACL-Liste eingetragene wireless Client diesen public key ebenfalls an der gleichen Stelle in seiner Schlüsselliste eingetragen haben wie der Access Point.

Beispiel

Ein Access Point verwendet in seiner Funkzelle zur Verschlüsselung des Datenverkehrs die Einstellung Shared Key mit einem 128 Bit public key (Default Key 1).

Alle Wireless Clients, die sich an diesen Access Point anmelden, benötigen diesen public key in ihrer Schlüsselliste an Position 1 zur Kommunikation.

Wird nun der Zugriff für bestimmte Wireless Clients über die ACL-Liste des Access Points auf Basis eines privaten Schlüssels eingeschränkt, muss zunächst der private Schlüssel in der Schlüsselliste des Access Points und der entsprechenden Wireless Clients hinterlegt werden.

Als nächstes werden die MAC-Adressen dieser Wireless Clients in die ACL-Liste des Access Points eingetragen und mit dem privaten Schlüssel versehen. Sollen diese Wireless Clients

weiterhin kommunizieren können, muss der private Schlüssel im Wireless Client direkt unter **Security->Basic->WLAN** für die Verschlüsselung eingestellt und verwendet werden. Ansonsten könnten die Clients nur Broad- oder Multicast-Pakete bekommen, jedoch nicht mehr direkt über Unicast-Pakete angesprochen werden.

Siehe auch

- Menüpunkt CLI\SECURITY\ACL\WLAN1 (bzw. \WLAN2 oder \WLAN3) (Seite 232)

5.6.5.5 Menüpunkt RADIUS Server

Hinweis

Der Menüpunkt "RADIUS" ist nur im Access Point-Modus verfügbar.

Authentifizierung über einen externen Server

Das Konzept von RADIUS basiert auf einem externen Authentifizierungs-Server. Für einen Client ist der Zugang zum Netzwerk erst möglich, nachdem der Access Point die Anmeldedaten des Clients beim Authentifizierungs-Server verifiziert hat. Sowohl der Client als auch der Authentifizierungs-Server müssen das EAP-Protokoll (Extensive Authentication Protocol) unterstützen. Der SCALANCE W-700 unterstützt die äußeren Authentifizierungs-Mechanismen EAP-TLS, EAP-TTLS und PEAP.

Siehe auch

- Menüpunkt CLI\SECURITY\RADIUS (Seite 233)

5.6.5.6 Menüpunkt Access

Zugriffsrechte für IP-Adressen

In diesem Menü bestimmen Sie Zugriffsrechte für IP-Adressen. Sie können festlegen, ob ein Management-Zugriff (SNMP, Telnet, WBM) mit den definierten Adressen möglich ist:

- Ein Management-Zugriff ist nur mit den definierten Adressen möglich.

Oder:

- Ein Management-Zugriff ist mit allen IP-Adressen möglich, die nicht in der Liste aufgeführt sind.

Hinweis

Die definierten Zugriffsrechte gelten auch für den PC, der für die Konfiguration verwendet wird. Wenn Sie die eigene IP-Adresse nicht eingetragen haben und den ACL-Modus auf "Accessed" gesetzt haben, ist ein weiterer Zugriff auf den SCALANCE W-700 nicht mehr möglich.

Beachten Sie außerdem, dass sich die IP-Adresse des Clients ändern kann, wenn Sie DHCP ohne Reservierung verwenden.

Siehe auch

- Menüpunkt CLI\SECURITY\ACCESS (Seite 234)

5.6.6 Das Menü Bridge

5.6.6.1 Menüpunkt Bridge

Einleitung

Unter einer Bridge versteht man eine Netzwerkkomponente, die zwei Netze miteinander verbindet. Eine Bridge arbeitet protokollunabhängig, das Management der Datenpakete erfolgt anhand der physikalischen Adresse der Netzteilnehmer (MAC-Adresse).

Der SCALANCE W-700 bietet eine Bridge-Funktionalität, weil er den Datenverkehr zwischen drahtgebundenem und drahtlosem Ethernet abwickelt. Die folgenden Abschnitte beschreiben, welche Funktionen zur Verfügung stehen und wie Sie diese konfigurieren und nutzen.

Löschen veralteter Bridge-Informationen

Der SCALANCE W-700 speichert die Information, welche MAC-Adresse über welchen Port erreicht werden kann, in der sogenannten Learning Table. Einträge in dieser Liste werden automatisch gelöscht, wenn für die entsprechenden MAC-Adressen kein Datentransfer mehr erfolgt. Nach welcher Zeit Adressen bei ausbleibendem Datenverkehr gelöscht werden, können Sie mit dem Parameter "Aging Time" auf der Startseite des Menüs "Bridge" festlegen.

Siehe auch

- Menüpunkt CLI\BRIDGE (Seite 235)

5.6.6.2 Menüpunkt WDS

Hinweis

Der Menüpunkt WDS ist nur im Access Point-Modus verfügbar und wenn iPCF nicht aktiviert ist

Kommunikation zwischen Access Points

Im normalen Betrieb ist der SCALANCE W78x als Schnittstelle zu einem Netz eingesetzt und kommuniziert mit Clients. Es gibt allerdings auch den Anwendungsfall, dass mehrere Access Points miteinander kommunizieren müssen, beispielsweise zum Zweck der Reichweitenvergrößerung oder zum Aufbau eines Wireless-Backbones. Diese Betriebsart ist mit WDS (Wireless Distributed System) möglich.

Hinweis

Nur für SCALANCE W788-xPRO/RR und W74x-1PRO/RR

Mit dem FW-Update auf ≥ V3.0 ist eine Nachkonfiguration für die Geräte SCALANCE W78x-xRR erforderlich, wenn Sie WDS oder Redundanz nutzen und dabei die MAC-Adresse und nicht die sysNamen benutzen.

Diese Funktionen basieren dann auf der MAC-Adresse, die sich durch die Einführung von VAPs mit der V3.0 änderte.

Konfiguration

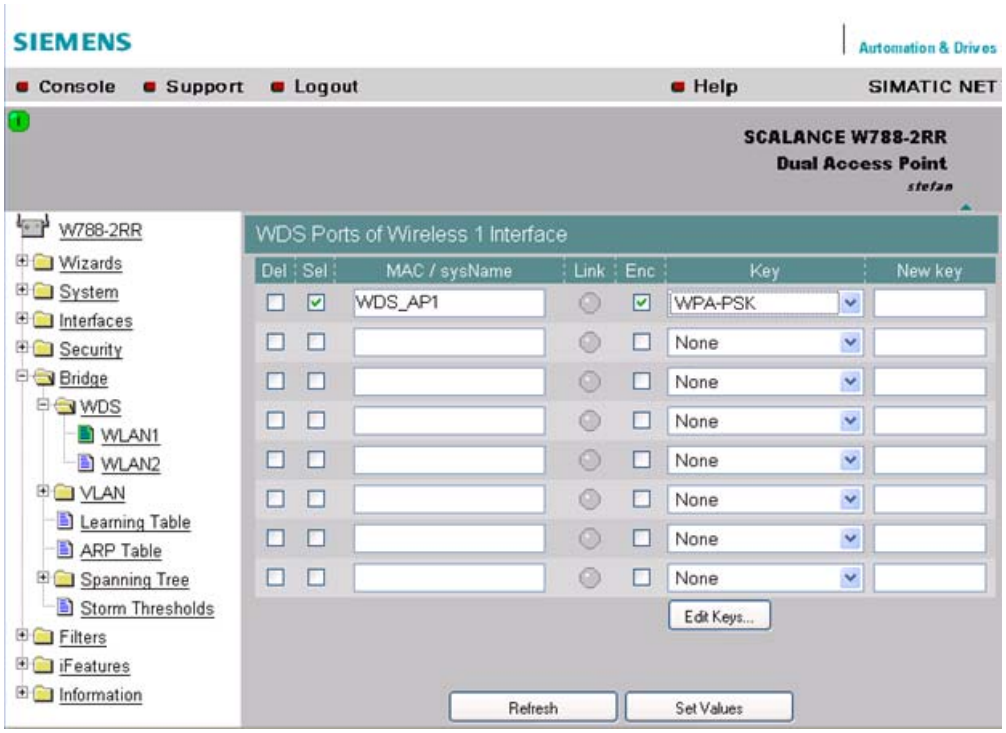
Tragen Sie in der Spalte "MAC / sysName" die MAC-Adresse oder den Systemnamen des Access Points ein, mit dem kommuniziert werden soll. Wenn Sie das Optionskästchen "Enc" markieren, wird Verschlüsselung angewendet.

Hinweis

Im WDS-Betrieb gelten folgende Einschränkungen:

- Alle Access Points, die miteinander kommunizieren sollen, müssen den gleichen Kanal benutzen.
- Als Verschlüsselungsverfahren können Sie entweder WEP oder WPA(2)_PSK auswählen.
  Falls Sie WPA_PSK oder WPA2_PSK als Verschlüsselungsverfahren benutzen wollen, müssen sie in den Security-Einstellungen den Modus WPA_PSK, WPA2_PSK oder WPA/WPA2-AUTOPSK sowie den WPA Passphrase im jeweiligen Interface (VAP0) einstellen. Ist eine andere Security-Stufe ausgewählt, können Sie bei WDS kein WPA(2)-PSK nutzen.
  Um WPA(2)-PSK zu aktivieren wählen Sie anstatt eines Schlüssels den Eintrag "WPA_PSK" aus.
  Sobald Sie bei einer Verbindung WPA-PSK oder WPA2-PSK gewählt haben, müssen Sie alle WDS-Verbindungen mit mindestens einem WEP-Schlüssel sichern.
- Wollen Sie einen anderen Access Point als den SCALANCE W78x über WDS anbinden, müssen Sie die MAC-Adresse konfigurieren. Das Erkennen über den Parameter "sysName" funktioniert in diesem Fall nicht.
- Im Übertragungsverfahren IEEE 802.11h ist es nicht sinnvoll, die Betriebsart WDS zu wählen. In der Betriebsart WDS müssen alle SCALANCE W78x den gleichen Kanal benutzen. Wird jetzt von einem Access Point ein Signal eines Primärnutzers entdeckt, wird der Kanal automatisch gewechselt und dadurch die bestehende Verbindung unterbrochen.
- Sobald Sie für mehrere WLAN-Schnittstellen den gleichen Kanal verwenden, müssen Sie die WDS-Adressierung unbedingt über MAC-Adressen vornehmen. Die Konfiguration über "sysName" kann ein Anmelden an der falschen Schnittstelle zur Folge haben, was die Kommunikation möglicherweise beeinträchtigt.

Damit der Eintrag aktiviert wird, müssen Sie das Optionskästchen "Sel" markieren.



Siehe auch

- Menüpunkt CLI\BRIDGE\WDS\WLAN1 (bzw. \WLAN2 oder \WLAN3) (Seite 236)

5.6.6.3 Menüpunkt VLAN

Hinweis

Der Menüpunkt "VLAN" ist nur im Access Point-Modus eines SCALANCE W78x verfügbar.

Zuordnung und Verwaltung der VLAN IDs

Die Maske "Current VLAN Configuration" zeigt die tabellarische Übersicht der konfigurierten VLAN IDs (VID). Des Weiteren wird die die Zuordnung der konfigurierten Ports des Access Points als Member zu diesen VLANs angezeigt.

Der "Name" dient nur der Identifizierung eines Eintrags innerhalb der aktuellen Tabelle. "Member List" zeigt 'U' für Untagged Member eines VLANs bzw. '–' falls ein Port nicht Mitglied eines VLANS ist. Die Abfolge ist von links nach rechts aufsteigend sortiert, d.h. nach der Kennung des Interfaces (WLAN 1, WLAN 1 VAP 1, WLAN 2 VAP 2… bzw. WLAN 1 WDS 1, WLAN 1 WDS 2...).

Rot markierte Einträge kennzeichnen in der Tabelle Member, schwarz markierte kennzeichnen die konfigurierten Port VLAN IDs.

Ist ein Interface Mitglied einer VLAN ID, die ungleich der Port VID ist, so werden vom Ethernet her eingehende Frames mit dieser VLAN ID angenommen. Ausgehenden Frames erhalten aber immer die Port VLAN ID.

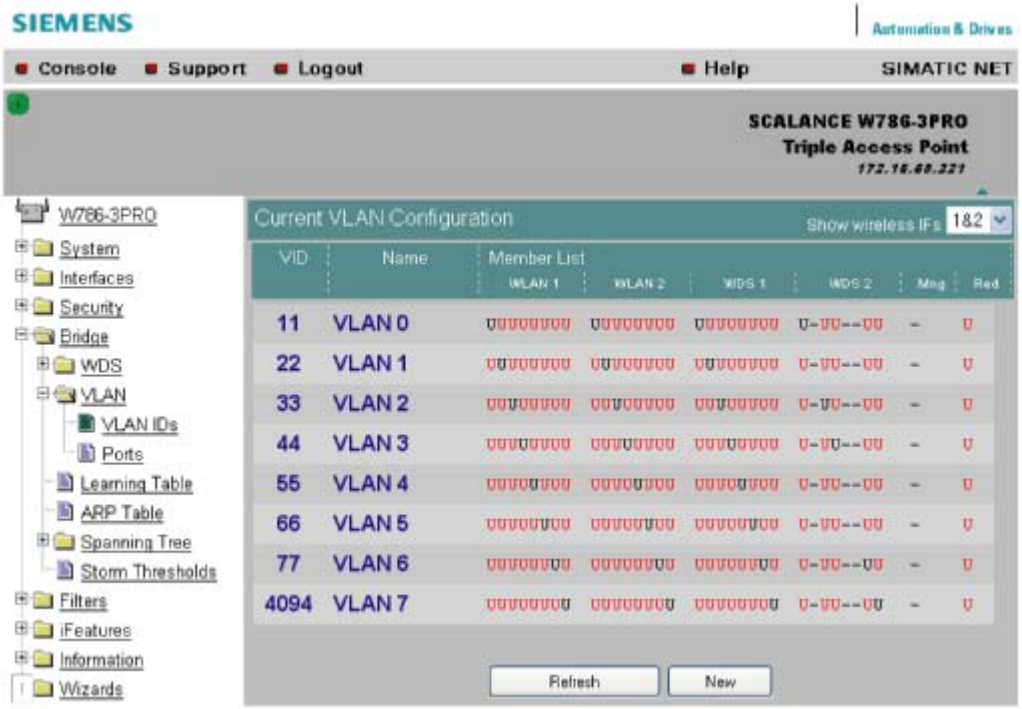
Klick auf "VID" oder "Name" führt zur Konfigurationsseite für VLAN IDs. Mit "New" wird eine neue VLAN ID angelegt, mit "Refresh" wird die Tabelle aktualisiert.

Hinweis

Das Ethernet Interface entfernt keine VLAN Tags von ausgehenden Frames.

Die WLAN Interfaces entfernen bei aktivem VLAN generell alle VLAN Tags von den ausgehenden Frames.

Member List	Bedeutung
U	Wenn VID gleich Port VID, d.h. ungetaggte Frames vom WLAN werden mit dieser VID versehen.
U	Wenn Port Mitglied der VID, d.h. getaggte Frames vom Ethernet werden auf diesem Port weitergeleitet.
—	Wenn Port nicht Mitglied der VID, d.h. es werden alle vom Ethernet kommenden Frames mit der ensprechenden VLAN ID geblockt/verworfen. Frames, die nicht konfigurierte VIDs enthalten und ungetaggte Frames werden bei aktivem VLAN generell geblockt.

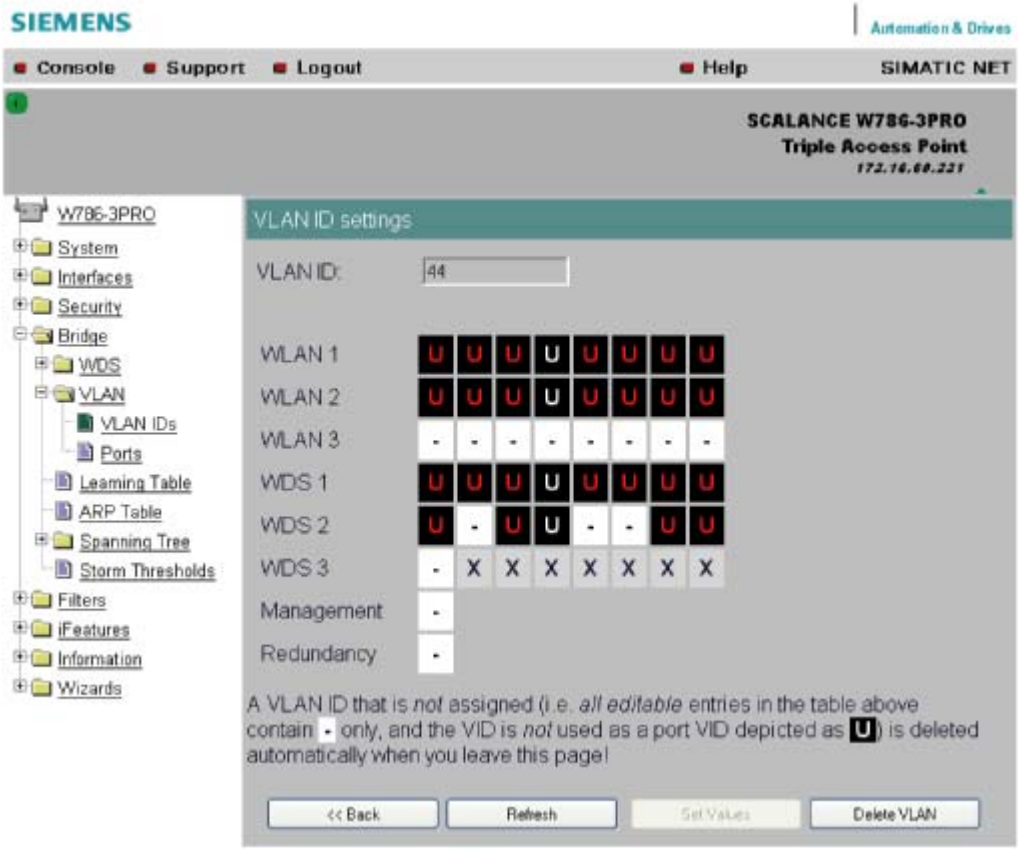


VLAN ID Einstellungen

Feld VLAN ID erlaubt den Eintrag einer neuen VID, solange kein Port explizit als Member zugeordnet ist. Andernfalls ist die VID nicht mehr änderbar.

Darstellung	Einstellungen	Bedeutung
1	-	Feld ist editierbar. Zeigen alle editierbaren Felder diese Darstellung und ist die VID nicht als Port VID konfiguriert, so wird beim Verlassen der Seite die VID gelöscht. Klick auf das Feld stellt auf Darstellung 2 um.
2	U	Feld ist editierbar. Klick auf das Feld stellt auf Darstellung 1 um.
3	-	Feld ist nicht editierbar. Alle Einträge für VLAN Membership sind belegt.
4	U	Feld ist nicht editierbar. VID entspricht der Port VID

Darstellung	Einstellungen	Bedeutung
5		Feld ist nicht editierbar. Entsprechender Port steht auf "all VIDs",
6		Feld ist nicht editierbar. Entsprechender Port ist nicht konfiguriert, daher kann keine VID zugeordnet werden.



Ports

Port: Tabellarische Übersicht der Ports.

"SSID": SSID für WLAN Iinterface, kein Eintrag für WDS bzw. Management und Redundanz.

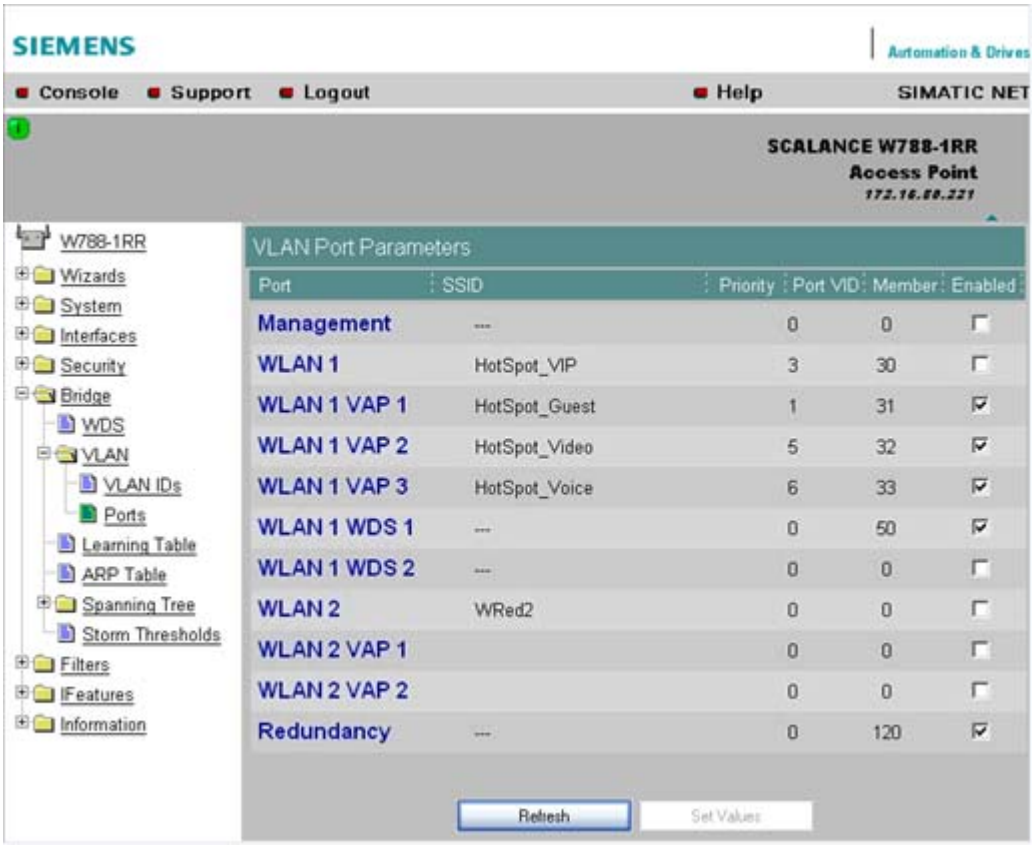
"Priority": Konfigurierte Priorität des Ports.

"Port VID": Direkt dem Port zugeordnete VLAN ID.

"Member": Die dem Port zugeteilte VLAN Membership.

"Enabled": Die VLAN Unterstützung kann direkt aktiviert / deaktiviert werden.

Klick auf einen Port führt zur Konfigurationsseite VLAN Settings.



Hinweis

Wenn Sie einen Radius Server zur Athentifizierung verwenden, muss dieser über das Management VLAN erreichbar sein. Der Management Port bedient unter anderem auch die Funktionen: HTTP, HTTPS, WBM, Telnet, SSH, Ping, DHCP, TFTP, SNMP, SNTP und Syslog.

Hinweis

Die IP- und MAC-basierten Teilnehmer hinter einem Client mit aktivierter Layer-2-Tunneling-Funktion (kurz: L2T-Client) übernehmen die gleichen VLAN-Eigenschaften, die der Client besitzt.

Beispiel: Ein L2T-Client ist mit dem Access Point über die Schnittstelle WLAN1 VAP3 verbunden. WLAN1 VAP3 ist Mitglied der VLAN ID 33, der die Priorität 6 zugeordnet ist. Damit ergibt sich für den L2T-Port, dass die angeschlossenen Geräte hinter dem L2T-Client und der Client selbst ebenfalls Mitglieder der VLAN ID 33 mit der Priorität 6 sind.

VLAN Einstellungen

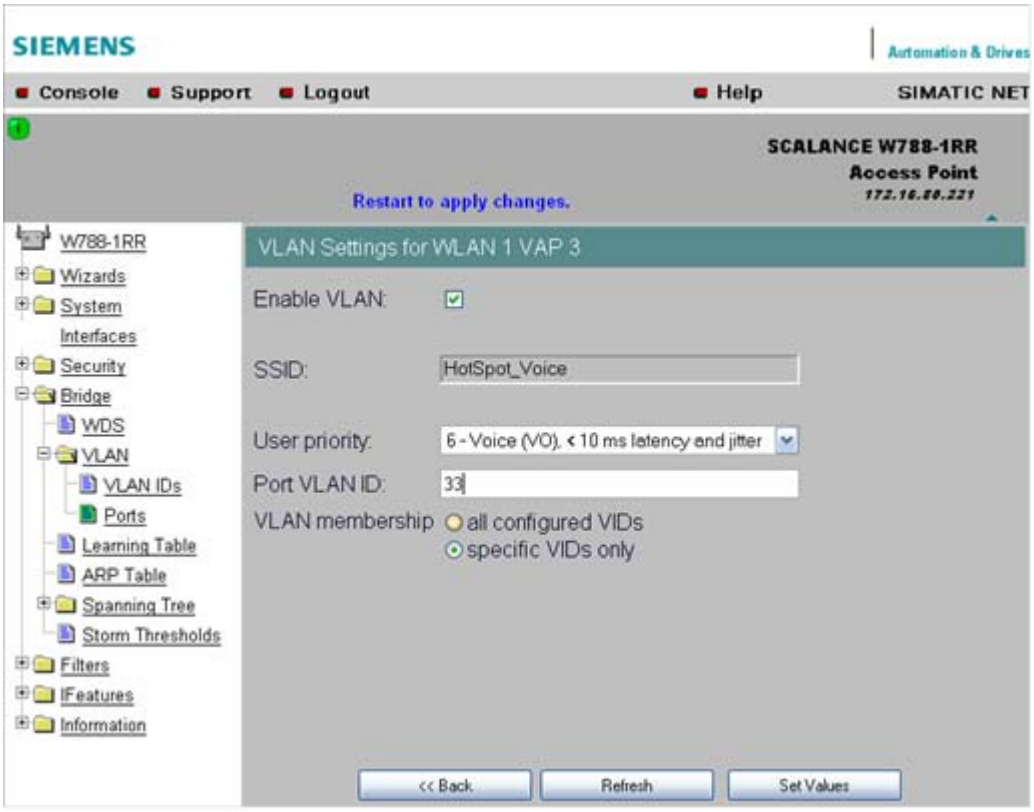
"VLAN enabled": Die VLAN Unterstützung kann direkt aktiviert / deaktiviert werden.

"User Priority": Priorisierung des Datenverkehrs über den Port. Ungetaggte Frames werden mit dieser Priorität versehen.

"Port VLAN ID": Eintrag der VLAN ID.

"VLAN Membership"
"All VIDs": Automatische Festlegung des Ports als Member aller konfigurierten VIDs.

"Specific VIDs only": Mitglied von bis zu acht frei zuordenbaren konfigurierten VIDs pro Port.



VLAN enable

Markieren Sie die Option "VLAN enable", wenn Sie die Funktion VLAN aktivieren wollen. Wenn "VLAN enable" aktiviert ist, werden alle Telegramme dieses VAP mit einem VLAN Tag versehen.

User priority

Legen Sie über das Klappliste "User priority" die Priorität der Telegramme dieses VAP fest. Die Priorität wird von den angeschlossenen VLAN-fähigen Switches (z.B. SCALANCE X-400) des Netzwerks ausgewertet. Die Priorität steigt mit aufsteigender Nummer:

Hinweis

Die Priorität steigt im Allgemeinen mit aufsteigender Nummer. Ausnahme ist die Priorität 0, die eine höhere Priorität als die Prio-Klassen 1 und 2 besitzt und gleichwertig zur Prio-Klasse 3 ist.

- "0 - Best Effort (BE)"
  Normaler Datenverkehr
- "1 - Background (BK)"
  Zeitunkritischer Datenverkehr
- "2 - Spare (--)"
  Diese Priorität ist reserviert.
- "3 - Excellent Effort (EE)"
  Datenverkehr mit höchster Priorität
- "4 - Controlled Load (CL)"
- "5 - Voice (VI), < 100 ms latency and jitter"
  Video/Multimedia
- "6 - Voice (VO), < 10 ms latency and jitter"
  Voice over IP
  PNIO
- "7 - Network Control (NC)"
  Interne Netzwerk-Steuertelegramme

Voreinstellung ist 0 - Best Effort (BE).

Hinweis

Sowohl Voice over IP als auch PNIO besitzen Priorität 6.

Port VLAN ID

Geben Sie hier die VLAN-Kennung (VID) desjenigen VLAN ein, auf dem der virtuelle Access Point kommunizieren soll.

Die einzelnen VLANs werden in den VLAN-fähigen Industrial Ethernet Switches (z.B. SCALANCE X-400) konfiguriert. Die VID eines VLAN liegt im Bereich von 1 bis 4094.

VLAN membership

Hier geben Sie an, bei welchen VLANs der virtuelle Access Point Mitglied sein soll bzw. welchen weiteren VLANs die oben eingetragene Port VLAN ID (VID) zugeordnet werden soll.

Folgende Alternativen der Zuordnung sind möglich:

- "all"
  Der VAP ist Mitglied aller VLANs.
- "only"
  Der VAP ist nur bei den im Folgenden eingetragenen VLANs Mitglied.

Tragen Sie hier die VLAN-Kennung (VID) von bis zu 8 VLANs ein, bei denen der VAP Mitglied sein soll.

Siehe auch

- Menüpunkt CLI\BRIDGE\VLAN\VLAN_ID (Seite 237)
- Menüpunkt CLI\BRIDGE\VLAN\PORTS (Seite 238)

5.6.6.4 Menüpunkt Learning Table

Zuordnung von MAC-Adresse und Port

Die Learning Table enthält die Angabe, ob eine MAC-Adresse über die drahtgebundene Ethernet-Schnittstelle oder über die drahtlose Schnittstellen erreicht werden kann. Diese Informationen leitet der SCALANCE W-700 aus dem laufenden Datenverkehr ab. Die Learning Table enthält auch die Informationen zu Clients und den bis zu acht dahinter angeschlossenen Geräten, die im Layer-2-Tunneling-Modus arbeiten.

5.6.6.5 Menüpunkt ARP Table

Zuordnung von MAC-Adresse und IP-Adresse

Das ARP-Protokoll (Address Resolution Protokoll) ermittelt bei bekannter IP-Adresse die zugehörige MAC-Adresse. Die Seite dieses Menüpunkts zeigt auch die Schnittstelle an, über die eine Adresse erreicht werden kann. Die letzte Spalte gibt an, wie die Information ermittelt wurde (beispielsweise "dynamic", wenn sie aus dem laufenden Betrieb abgeleitet wurde, oder "static", falls sie fest konfiguriert worden ist).

5.6.6.6 Menüpunkt Spanning Tree

Hinweis

Der Menüpunkt "Spanning Tree" ist nur verfügbar, wenn Sie den SCALANCE W78x im Access Point-Modus verwenden.

Vermeidung von Schleifenbildung bei redundanten Verbindungen

Das Spanning Tree-Verfahren ermöglicht es, Netzwerkstrukturen aufzubauen, bei denen es mehrere Verbindungen zwischen zwei Stationen gibt. Spanning Tree verhindert, dass es zu einer Schleifenbildung im Netz kommt, in dem es genau einen Pfad zulässt und die anderen (redundanten) Ports für den Datenverkehr deaktiviert. Bei einer Unterbrechung können die Daten über einen alternativen Pfad gesendet werden. Die Funktionalität des Spanning Tree-Verfahrens basiert auf dem Austausch von Konfigurations- und Topologieänderungs-Telegrammen.

Definition der Netztopologie durch Konfigurationstelegramme

Netzwerkkomponenten tauschen zur Berechnung der Topologie untereinander Konfigurations-Telegramme aus, so genannte BPDUs (Bridge Protocol Data Unit). Mit diesen Telegrammen wird die Root Bridge ausgewählt und die Netztopologie erstellt. Die Root Bridge ist die Bridge, die das Spanning Tree-Verfahren für alle beteiligten Komponenten steuert. Darüber hinaus bewirken BPDU-Telegramme den Statuswechsel der Bridge-Ports.

Rapid Spanning Tree

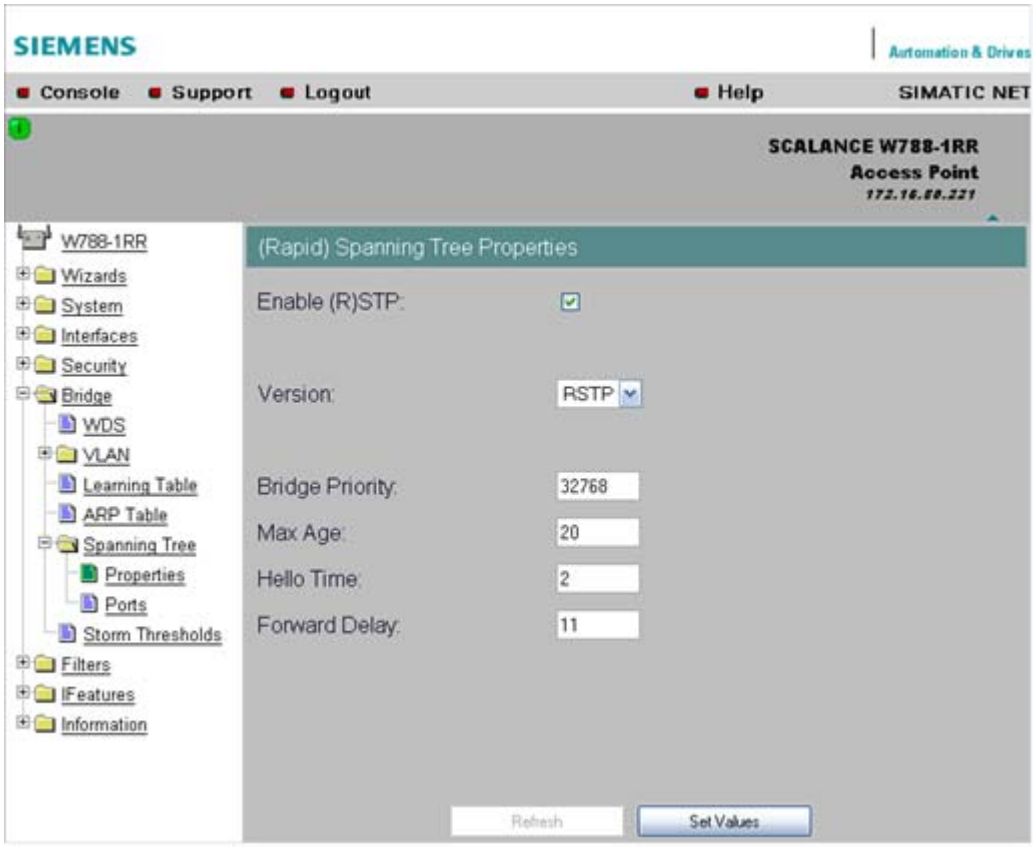
Das Rapid Spanning Tree-Verfahren basiert auf dem Spanning Tree-Verfahren. Es wurde in Bezug auf die Rekonfigurationszeit optimiert.Typische Rekonfigurationszeiten bei Spanning Tree liegen zwischen 20 und 30 Sekunden. Bei Rapid Spanning Tree liegen die Rekonfigurationszeiten im Sekundenbereich. Das wird durch folgende Maßnahmen erreicht:

- Edge Ports (Endteilnehmer-Port)
  Ein Port, der als Edge Port definiert ist, wird schon nach Ablauf der Hello Time (dem Zeitabstand zwischen zwei Konfigurationstelegrammen) aktiv geschaltet. Nach Ablauf der Hello Time kann die Station sicher sein, dass kein Konfigurationstelegramm mehr kommt, und es handelt sich bei diesem Port um einen Endteilnehmer. Will der Anwender auch die Hello Time vermeiden, dann kann an diesem Port Spanning Tree deaktiviert werden.
- Point to Point (direkte Kommunikation zweier benachbarter Stationen)
  Durch die direkte Koppelung von Netzwerkkomponenten kann eine Zustandsänderung (Umkonfiguration der Ports) ohne Verzögerungen durchgeführt werden. Eine Point to Point Verbindung kann zum Beispiel eine WDS-Verbindung zwischen zwei Access Points sein.
- Alternate Port (Ersatz für den Root-Port)
  Es ist ein Ersatz für den Root-Port konfiguriert. Bei einem Verbindungsverlust zur Rootbridge kann die Station deshalb ohne Verzögerung durch Neukonfiguration eine Verbindung über den Alternate Port aufbauen.
- Filtertabelle
  Bei Rapid Spanning Tree werden Ports, die von einer Umkonfiguration betroffen sind, sofort aus der Filtertabelle gelöscht. Im Gegensatz dazu ist bei Spanning Tree der Zeitpunkt des Eintrages in die Filtertabelle für das Löschen von Ports maßgeblich.
- Reaktion auf Ereignisse
  Rapid Spanning Tree reagiert auf Ereignisse, beispielsweise einen Verbindungsabbruch, ohne Verzögerung. Es müssen also keine Zeitgeber wie bei Spanning Tree abgewartet werden.

Prinzipiell werden also bei Rapid Spanning Tree für viele Parameter Alternativen vorkonfiguriert oder bestimmte Eigenschaften der Netzstruktur berücksichtigt, um die Rekonfigurationszeit zu verkürzen.

(Rapid) Spanning Tree-Konfiguration

Die für das (Rapid) Spanning Tree-Protokoll verwendeten Parameter werden im Menüpunkt "(Rapid) Spanning Tree Properties" angezeigt.



Verändern Sie gegebenenfalls die folgenden Parameter, um das Betriebsverhalten des (Rapid) Spanning Tree Algorithmus zu beeinflussen:

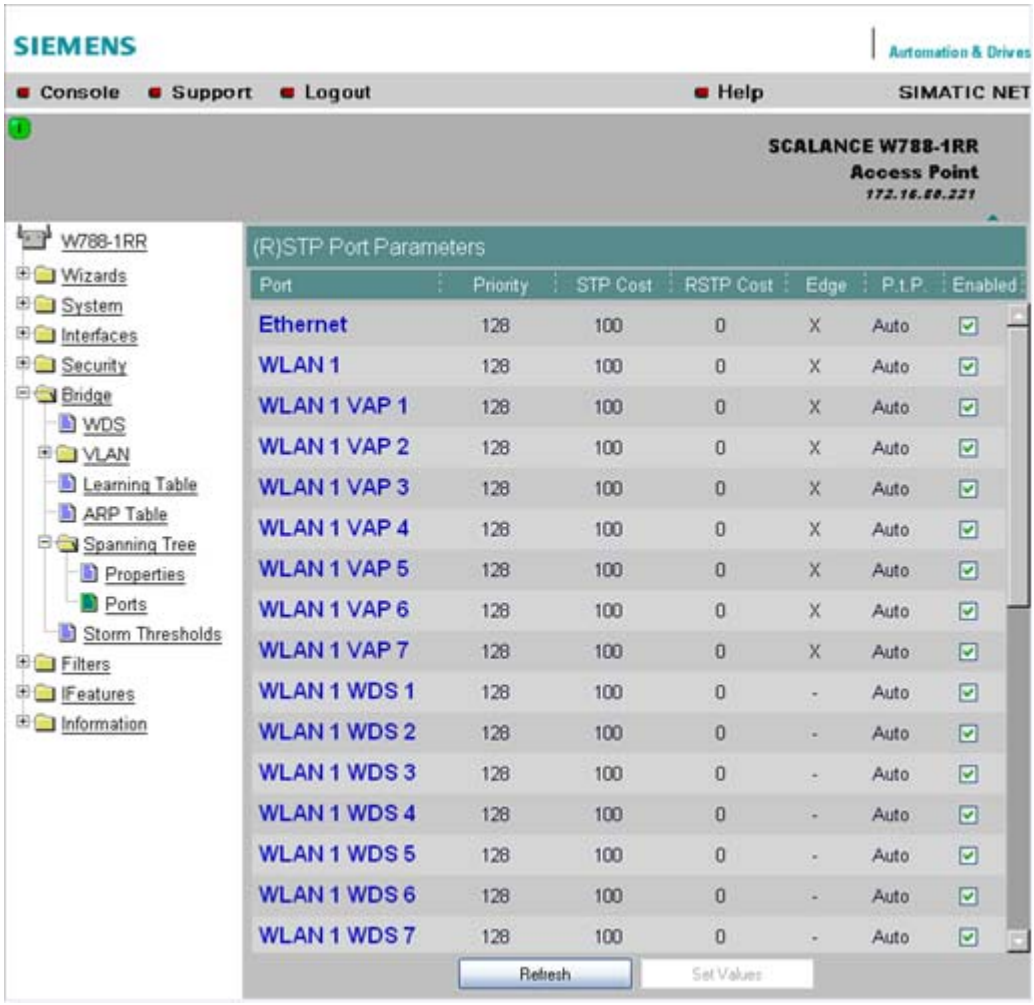
- Optionskästchen Enable (R)STP
  Markieren Sie das Optionskästchen Enable Spanning Tree, wenn Sie den (Rapid) Spanning Tree-Algorithmus nutzen wollen. Ist das Häkchen nicht gesetzt sind alle Ports automatisch im Zustand ‚Forwarding'.
- Klappliste Version
  Anhand der Version wird festgelegt, ob das Rapid Spanning Tree Protokoll (RSTP) verwendet oder das Gerät im Kompatibilitätsmodus des Spanning Tree Protokolls (STP) betrieben werden soll.
- Eingabefeld Bridge Priority
  Die Ermittlung der effizientesten Verbindung erfolgt immer im Bezug auf die sogenannte Root Bridge, einer Netzkomponente, die als Wurzelelement einer baumartigen Netzstruktur angesehen wird. Mit dem Parameter "Bridge Priority" können Sie die Wahl der Root Bridge beeinflussen.
  Die Bridge mit der höchsten Priorität (d. h. dem kleinsten Wert für diesen Parameter) wird Root Bridge. Wenn in einem Netz mehrere Netzwerk-Komponenten die gleiche Priorität besitzen, dann wird die Station zur Root Bridge, deren MAC-Adresse den niedrigsten Zahlenwert hat. Beide Parameter, Bridge Priority und MAC-Adresse, bilden zusammen den Bridge Identifier. Da die Root Bridge alle Wegeänderungen verwaltet, sollte sie wegen der Laufzeit der Telegramme möglichst zentral angeordnet sein. Der Wert für die Bridge Priority ist ein ganzzahliges Vielfaches von 4096 in einem Wertebereich von 0 bis 61440.

- Eingabefeld Max Age
  Max Age ist die Zeit, die eine Bridge auf ein Konfigurations-Telegramm (BPDU) wartet. Wenn die Zeit vorbei ist, versucht die Bridge das Netz zu rekonfigurieren. Der Default-Wert für diesen Parameter beträgt 20 Sekunden.
- Eingabefeld Hello Time
  Jede Bridge versendet regelmäßig Konfigurationstelegramme (BPDUs). Der Zeitabstand zwischen zwei solchen Telegrammen ist die "Hello Time". Der Default-Wert für diesen Parameter beträgt 2 Sekunden.
- Eingabefeld Forward Delay
  Neue Konfigurationsinformationen werden von einer Bridge nicht sofort, sondern erst nach dem im Parameter Forward Delay festgelegten Zeitraum angewendet. So wird sichergestellt, dass der Betrieb entsprechend der neuen Topologie erst gestartet wird, wenn alle Bridges die notwendigen Informationen haben. Der Default-Wert für diesen Parameter beträgt 15 Sekunden.

Spanning Tree Port Einstellungen

Portspezifische Parameter

Diese Seite zeigt die aktuellen Port-Parameter. Die Einstellungen erfolgen entweder über die Autofunktion des SCALANCE W-700 oder durch den Anwender.



Die acht Spalten der Port-Tabelle zeigen folgende Informationen:

- Port
  Angabe des Ports, auf den sich die Informationen beziehen. Die Angabe WLAN1 VAP2 bezieht sich zum Beispiel auf den Virtuellen Access Point VAP2 an der ersten WLAN-Schnittstelle.
- Priority
  Sie legen mit diesem Parameter die Priorität der Ports einer Bridge fest.
  Kann der von Spanning Tree ermittelte Weg alternativ über mehrere Ports einer Station führen, so wird der Port mit der höchsten Priorität (d. h. dem kleinsten Wert für diesen Parameter) ausgewählt. Für die Priorität kann ein Wert von 0 bis 240 angegeben sein, der Default-Wert ist 128.
- STP Cost & RSTP
  Diese Parameter dienen zur Berechnung des zu wählenden Weges. Je geringer dieser Wert ist, umso größer ist die Wahrscheinlichkeit, dass bei der Wegewahl die entsprechende Strecke berücksichtigt wird. Haben mehrere Ports einer Bridge den gleichen Wert, wird der Port, mit der niedrigsten Portnummer ausgewählt. Je nachdem, ob als Version STP oder RSTP ausgewählt worden ist, wird der Wert von STP Cost oder

RSTP Cost verwendet.
Die Ermittlung der Pfadkosten richtet sich maßgeblich nach der Übertragungsgeschwindigkeit. Je höher die erzielbare Übertragungsgeschwindigkeit ist, umso kleiner sollte der Wert für Path Cost sein.
Typische Pfadkosten für Spanning Tree und Rapid Spanning Tree:
(Die Werte können aber auch individuell parametriert werden.)

Datenrate	Pfadkosten STP	Pfadkosten RSTP
100 Mbit/s	19	200.000
54 Mbit/s	33	370.370
48 Mbit/s	36	416.667
36 Mbit/s	43	555.556
24 Mbit/s	53	833.333
18 Mbit/s	58	1.111.111
12 Mbit/s	83	1.666.667
11 Mbit/s	90	1.818.182
10 Mbit/s	100	2.000.000
9 Mbit/s	111	2.222.222
6 Mbit/s	166	3.333.333
5,5 Mbit/s	181	3.636.364
2 Mbit/s	500	10.000.000
1 Mbit/s	1000	20.000.000

- Edge
  In dieser Spalte sind folgende Eintragungen möglich:
  yes An diesem Port befindet sich ein Endgerät.
  no An diesem Port befindet sich ein Spanning Tree- oder Rapid Spanning Tree-Gerät.
  Bei einem Endgerät kann ein SCALANCE W-700 ohne Rücksicht auf Spanning Tree-Telegramme schneller den Port umschalten. Wird entgegen dieser Einstellung ein Spanning Tree-Telegramm empfangen, dann wechselt der Port automatisch auf die Einstellung no für weitere Stationen.

Hinweis

Verbinden sich Clients mit aktivierter Layer-2-Tunneling-Funktion mit dem Access Point, wird für jeden dieser Clients ein eigener Port eröffnet. Diese Ports sind jedoch nicht für Rapid Spanning Tree konfigurierbar. Es werden die Einstellungen (z.B. Priorität und Pfadkosten etc.) der Funkzelle übernommen, über die der Client mit dem Access Point verbunden ist.

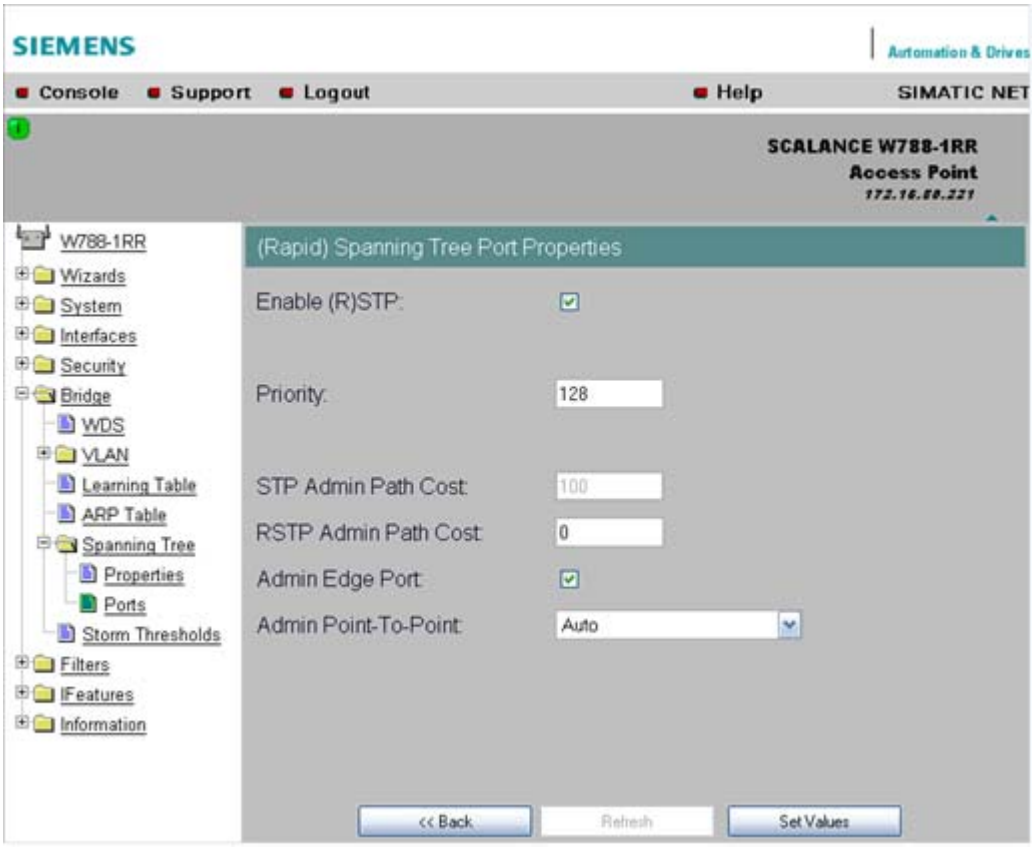
Beispiel: Ein L2T-Client ist über die Schnittstelle WLAN1 VAP3 mit dem Access Point verbunden. Für WLAN1 VAP3 wurde die Priorität 128, Pfadkosten für STP von 100, Pfadkosten für RSTP von 0 und die Einstellung EdgePort aktiv (d.h. an diesem Port befindet sich ein Endgerät) parametriert. Diese Einstellungen werden für den L2T-Port übernommen, bis auf eine Ausnahme.

Die Einstellung Edge-Port aktiv wird nicht übernommen, weil Layer-2-Tunneling-Clients und die Teilnehmer hinter dem Client nie Edge-Ports werden können.

- P.t.P.
  Eine Point to Point-Verbindung liegt dann vor, wenn zwei RSTP-fähige Netzkomponenten über diesen Port miteinander verbunden sind. Es gibt 3 mögliche Zustände:
  - ForceTrue
    Auch bei Halbduplex wird von einer direkten Verbindung ausgegangen.
  - ForceFalse
    Trotz einer Vollduplexverbindung wird nicht von einer Point to Point-Verbindung ausgegangen.
  - Auto
    Point to Point wird automatisch ermittelt. Steht der Port auf Halbduplex (Shared Media Connection), wird nicht von einer direkten Verbindung ausgegangen.
  - Beispiel: Eine WDS-Verbindung zwischen zwei Access Points ist immer eine Halbduplexverbindung. Bei der Einstellung ForceTrue wird von einer direkten Verbindung ausgegangen. Bei Auto würde nicht von einer direkten Verbindung ausgegangen.
- Enabled
  Zeigt an, ob Spanning Tree für den Port aktiviert (enabled) oder deaktiviert (disabled) ist.

Konfiguration eines Ports für (Rapid) Spanning Tree

Wenn Sie in der ersten Spalte eine Portbezeichnung anklicken, gelangen Sie zur Seite "(Rapid) Spanning Tree Port Properties":



Optionskästchen "Enable (R)STP"
Aktivieren Sie diese Option, wenn der Port das (Rapid) Spanning Tree-Protokoll verwenden soll.

- Eingabefeld "Priority"
  Geben Sie hier einen Wert zwischen 0 und 240 für die Port-Priorität ein.
- Eingabefeld "Admin Path Cost"
  Hier können Sie einen Wert für den Parameter STP bzw. RSTP Path Cost eingeben. Je nach ausgewählter Version wird dann der zugehörige Wert verwendet.
  Wenn Sie eine Null für den RSTP Wert eintragen, wird der Wert für die Pfadkosten automatisch berechnet.
- Optionskästchen "Admin Edge Port"
  Aktivieren Sie diese Option, wenn sich an diesem Port ein Endgerät befindet, andernfalls wird bei jeder Linkänderung an diesem Port eine Rekonfiguration des Netzwerkes ausgelöst.
- Klappliste "Admin Point to Point Status"
  Hierfür gibt es drei Einstellmöglichkeiten:
  - Shared media Connection ist markiert:
    Dies entspricht der Angabe "ForceFalse" in der Porttabelle.
  - Point to Point Connection ist markiert:
    Dies entspricht der Angabe "ForceTrue" in der Porttabelle.
  - Point to Point Connection und Shared Media Conection sind nicht markiert:
    Dies entspricht der Angabe "Auto" in der Porttabelle.

  Hinweis

  Punkt zu Punkt zu Punkt bedeutet eine direkte Verbindung zwischen zwei Stationen. Shared Media Connection wäre z.B. eine Verbindung vom Ethernetport zu einem Hub oder eine WDS-Verbindung zwischen zwei Access Points.

Siehe auch

- Menüpunkt CLI\BRIDGE\SPANNING (Seite 239)
- Menüpunkt CLI\BRIDGE\SPANNING\PORTS (Seite 240)

5.6.6.7 Menüpunkt Storm Threshold

Hinweis

Der Menüpunkt "Storm Threshold" ist im Access Point- und im Client-Modus verfügbar. Die Funktion kann im Client-Modus nur verwendet werden, wenn NAT deaktiviert ist.

Begrenzung von Broadcast- und Multicast-Telegrammen

Storm Threshold ist das Maximum an Broadcast- oder Multicast-Telegramme pro Sekunde, das der SCALANCE W-700 weiterleitet. Wird dieser Grenzwert überschritten, verarbeitet der SCALANCE W-700 solche Telegramme 30 Sekunden lang nicht mehr.

Siehe auch

- Menüpunkt CLI\BRIDGE\STORMTHR (Seite 241)

5.6.6.8 Menüpunkt NAT

Hinweis

Dieser Menüpunkt ist nur bei den folgenden Modellvarianten verfügbar:

- SCALANCE W746-1PRO
- SCALANCE W746-1
- SCALANCE W747-1RR
- SCALANCE W747-1
- SCALANCE W78x (nur im Client-Modus)

Was ist NAT?

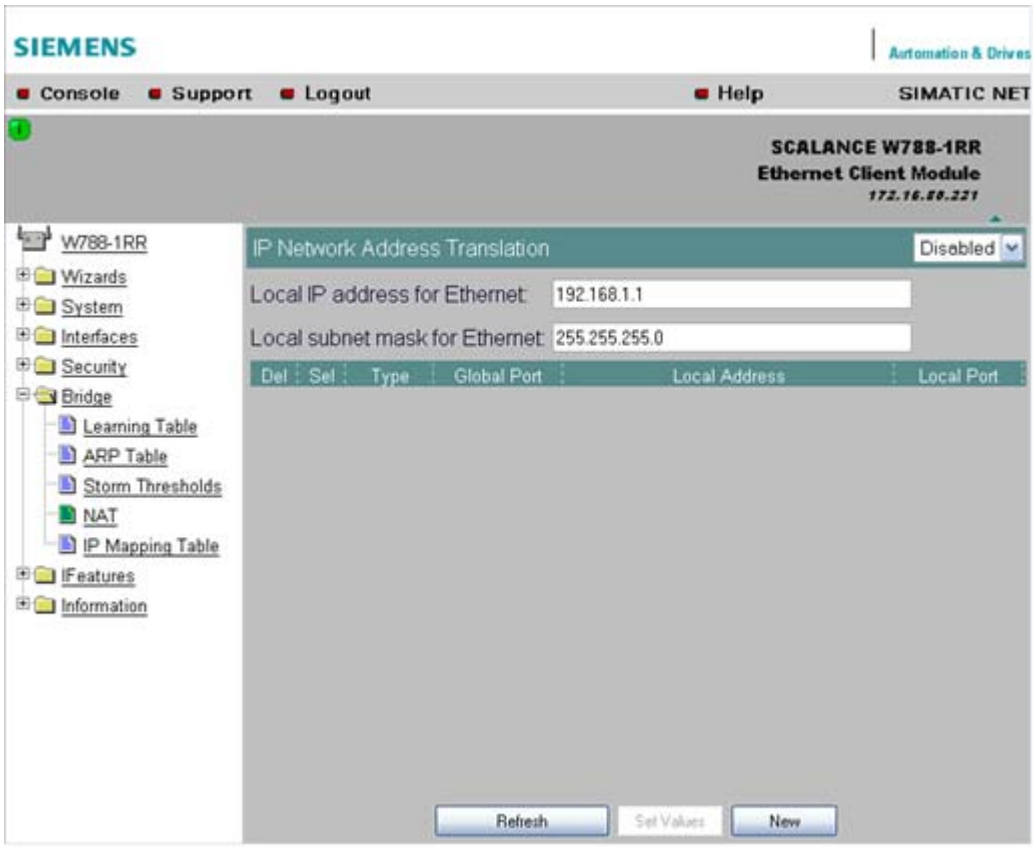
Mit Network Address Translation (NAT) wird die IP-Adresse in einem Datenpaket durch eine andere ersetzt. NAT wird in der Regel an einem Netzübergang zwischen einem privaten LAN und einem externen Netz mit global gültigen IP-Adressen eingesetzt. Dabei wird eine lokale IP-Adresse des internen LAN von einem NAT-Gerät am Netzübergang in eine externe, globale IP-Adresse umgeschrieben.

Zur Übersetzung der internen in die globale IP-Adresse pflegt das NAT-Gerät eine Übersetzungsliste.

Was ist NAPT?

Bei "Network Address Port Translation" (NAPT) oder "Port Address Translation" (PAT) werden mehrere interne Quell-IP-Adressen in die gleiche externe Quell-IP-Adresse umgeschrieben. Zur Identifikation der einzelnen Quell-Teilnehmer wird auch der Port des Quellgeräts in der Übersetzungsliste des NAT-Gateways gespeichert und für die externe Adresse umgeschrieben.

Wenn mehrere lokale Clients über das NAT-Gateway eine Anfrage an die gleiche externe Ziel-IP-Adresse senden, trägt das Gateway jeweils seine eigene externe Quell-IP-Adresse in den Header dieser weitergeleiteten Telegramme ein. Da die weitergeleiteten Telegramme die gleiche globale Quell-IP-Adresse haben, ordnet das NAT-Gateway die Telegramme den Clients über eine unterschiedliche Port-Nummer zu.



Hinweis

NAT/NATP ist nur auf Schicht 3 des ISO/OSI-Referenzmodells möglich. Zur Nutzung der NAT-Funktion müssen die Netze das IP-Protokoll verwenden.

Bei Verwendung des ISO-Protokolls, das auf Schicht 2 arbeitet, ist keine Nutzung von NAT möglich.

NAT-Eigenschaften der SCALANCE-Geräte

Bei Einsatz der folgenden WLAN-Clients als NAT-Gateway müssen die WLAN-Clients über die Ethernet-Schnittstelle mit den lokalen Ethernet-Devices verbunden werden:

- SCALANCE W746-1PRO
- SCALANCE W746-1
- SCALANCE W747-1RR
- SCALANCE W747-1
- W78x (im Client-Modus)

In den Ethernet-Devices muss die lokale IP-Adresse des WLAN-Clients als Gateway-Adresse eingetragen werden.

Die Adress-Zuordnung unterscheidet sich nach der Kommunikationsrichtung:

- Vom Ethernet-Device zum Access Point: "Dynamische" Adress-Zuordnung (NAT)
  Die fortlaufende Adress-Zuordnung erfolgt automatisch.
- Vom Access Point zum Ethernet-Device: "Statische" Adress-Zuordnung (NAPT)
  Die Adress-Zuordnung ist fest und muss parametriert werden.

Pro WLAN-Client als NAT-Gateway sind 32 Einträge parametrierbar.

Konfiguration

Nehmen Sie zur Konfiguration auf der Seite IP Network Address Translation folgende Einstellungen vor:

- Enable NAT
  Klicken Sie das Optionskästchen "Enable" an, wenn Sie NAT aktivieren wollen.
  Achtung: Für die Übernahme der Änderung wird ein Neustart angefordert!
- Local IP
  Geben Sie hier die lokale IP-Adresse für die Ethernet-Schnittstelle des WLAN-Clients ein.
- Subnet Mask
  Geben Sie hier ggf. eine Subnetzmaske für das lokale Ethernet ein.
- Del
  Klicken Sie das Optionskästchen "Delete" an, wenn Sie alle bisherigen Einträge in dieser Seite löschen wollen.
- Sel
  Klicken Sie das Optionskästchen "Select" an, wenn Sie die aktuellen Einträge aktivieren wollen.
- Type
  Wählen Sie hier die Zuordnung TCP oder UDP für den folgenden globalen Port. TCP- und UDP-Telegramme sind separat zu parametrieren.
- Global Port
  Geben Sie hier die Nummer des globalen Ports (für TCP oder UDP) ein.

Hinweis

Wenn der Port bereits durch einen lokalen Dienst (z. B. Telnet) belegt ist, dann wird eine Warnmeldung ausgegeben. Vermeiden Sie auf jeden Fall die Nutzung von Port 23 (Telnet), Port 22 (SSH) und die Ports 80/443 (http/https: Erreichbarkeit des Clients mit dem WBM) als globalen Port.

- Local Address
  Geben Sie hier die lokale IP-Adresse des Ethernet-Device ein.
- Local Port
  Geben Sie hier die Nummer des lokalen Ports des Ethernet-Device ein.

Hinweis

Die folgenden Hinweise gelten nur für die IP-Parametrierung über PST-Tool.

Bei PST-Zugriff auf die Baugruppe mit einem Projektierungsrechner erfolgt je nach Schnittstelle eine unterschiedliche Adress-Zuordnung:

- PST über die Wireless-Schnittstelle:
  Es erfolgt eine Änderung der "globalen" Adresse.
- PST über die Ethernet-Schnittstelle:
  Es erfolgt eine Änderung der "lokalen" Adresse.

Siehe auch

- Menüpunkt CLI\BRIDGE\NAT (Seite 241)
- Menüpunkt CLI\BRIDGE\NAT\STATIC (Seite 243)

5.6.6.9 Menüpunkt IP Mapping Table

Hinweis

Dieser Menüpunkt ist nur bei den folgenden Modellvarianten verfügbar:

- SCALANCE W746-1PRO
- SCALANCE W746-1
- SCALANCE W747-1RR
- SCALANCE W747-1
- SCALANCE W78x im Client-Modus

Hinweis

IP-Mapping-Tabelle

Ist bei einem Client Layer 2 Tunneling konfiguriert, wird die IP-Mapping-Tabelle nicht angezeigt.

WLAN-Zugang mehrerer Geräte über einen Client

Mit den im ersten Absatz genannten Geräten können Sie mit einem Client mehreren Geräten den WLAN-Zugang ermöglichen. So brauchen Sie nicht jedes Gerät mit einem eigenen Wireless-Client auszustatten.

Voraussetzung für dieses sogenannte IP-Mapping ist, dass die angeschlossenen Geräte nur mit IP-Telegrammen angesprochen werden sollen. Eine Kommunikation auf MAC-Adressen-Ebene (ISO/OSI Schicht 2) kann

- zu einer Komponente erfolgen, deren MAC-Adresse im Client konfiguriert ist,
- zu maximal acht Komponenten erfolgen, wenn die Funktion Layer-2-Tunneling gewählt wird.

Die Einstellung Layer-2-Tunneling erfüllt Forderungen von Industrie-Applikationen, bei denen MAC-Adressen basierte Kommunikation zu mehreren Geräten hinter dem Client stattfindet. Clients mit dieser Einstellung können sich nicht auf Standard-Wifi-Geräte und Access Points mit Firmware V3.0 oder älter verbinden.

MAC Mode

IP-Telegramme in Richtung vom Client zum Access Point enthalten als Source-MAC-Adresse die MAC-Adresse des WLAN-Interfaces. Somit stehen in den ARP-Tabellen auf der Access Point-Seite immer nur die MAC-Adresse des WLAN Interfaces der Clients.

Sind hinter dem Client mehrere Geräte, sollte nicht die Option Auto Find 'Adopt MAC' aktiviert sein. In diesem Falle würde die MAC-Adresse wahllos an das erste Gerät vergeben, das sich über Ethernet meldet.

Wenn zwischen dem Access Point und dem Client nur IP-Kommunikation stattfindet, kann die Default-Einstellung "AdoptOwnMAC" beibehalten werden. Sollen MAC-Adressen

basierte Telegramme auch von Geräten hinter dem Client versendet werden können, müssen Sie die Einstellungen Adopt MAC manually,

Autofind Adopt MAC oder Layer-2- Tunneling auswählen.

Zuordnung MAC-Adresse/IP-Adresse

Der Client unterhält eine Tabelle mit der Zuordnung von MAC-Adresse und IP-Adresse, um eingehende IP Telegramme an die richtige MAC-Adresse zu verschicken. Der Menüpunkt "IP Mapping Table" zeigt diese Tabelle. Prinzipiell können hinter einem Client beliebig viele Geräte mittels IP erreicht werden. Der Client kann bis zu acht Geräte verwalten. Beim Hinzukommen eines neuen Gerätes wird der älteste Eintrag aus der Tabelle gelöscht und damit Platz für den neuen Eintrag geschaffen. Da der Datendurchsatz einer drahtlosen Verbindung nicht beliebig erhöht werden kann, sollten maximal acht Geräte von einem Client verwaltet werden.

Siehe auch

- Adopt MAC Address Einstellungen (Nur für Clients oder Access Points im Client-Modus) (Seite 83)

5.6.7 Das Menü Filters

5.6.7.1 Menüpunkt Filters

Hinweis

Das Menü "Filter" sowie die zugehörigen Menüpunkte sind nur verfügbar, wenn Sie den SCALANCE W78x im Access Point-Modus verwenden. Die Betriebsart können Sie im Menü "System" festlegen.

5.6.7.2 Menüpunkt MAC Filters

MAC-Filter

Bei aktiviertem MAC-Filter ist eine Kommunikation mit Clients auf der Ethernetseite nur möglich, wenn deren Source-MAC-Adresse in der Tabelle eingetragen ist. Alternativ ist eine Einstellung möglich, bei der für alle angegebenen MAC-Adressen der Zugriff verweigert wird. Sie können maximal 50 MAC-Adressen in die Tabelle eintragen.

Beim IP-Mapping eines SCALANCE W78x im Client-Modus ist nur die für dieses Gerät vergebene MAC-Adresse relevant, die MAC-Adressen der dahinterliegenden Geräte auf Ethernet-Seite spielen bei der Filterung keine Rolle.

Ist das Optionskästchen "WDS" aktiviert, wird auch über die WDS-Ports gefiltert.

Siehe auch

- Menüpunkt CLI\FILTERS\MAC1FLT (Seite 244)

5.6.7.3 Menüpunkt MAC Dir Filter

Einschränkung des Datenverkehrs zwischen MAC-Adressen

Für Wireless Clients, die am Access Point angebunden sind, kann eine Filterung des gerichteten Datenverkehrs durchgeführt werden. Dieser Filter dient dazu, einer bestimmten MAC-Adresse nur Zugang zu bestimmten anderen MAC-Adressen zu erlauben. Sie können für eine Zieladresse mehrere Quelladressen bzw. Einträge angeben. Die Kommunikation der Zieladresse ist dann auf diese Einträge beschränkt. Für Zieladressen, die nicht im Filter eingetragen worden sind, gibt es keine Restriktionen.

Siehe auch

- Menüpunkt CLI\FILTERS\MAC2FLT (Seite 245)

5.6.7.4 Menüpunkt Protocol Filter

Protokollauswahl

Ohne Protokollfilterung verarbeitet der SCALANCE W78x alle Datenpakete, unabhängig vom verwendeten Protokoll. Aus Gründen der Datensicherheit und zur Lastverminderung kann es jedoch zweckmäßig sein, die Kommunikation über bestimmte Protokolle zu verhindern.

Dabei sind sie nicht auf die Protokolle beschränkt, die in der Liste dieses Menüpunkts enthalten sind. Bei Bedarf können Sie die Liste um eigene Einträge ergänzen. Sie können maximal 50 Ethernet II Protokolle festlegen, für die eine Filterung erfolgen soll.

Siehe auch

- Menüpunkt CLI\FILTERS\PROTO (Seite 246)

5.6.8 Das Menü I-Features

5.6.8.1 Menüpunkt I-Features

Hinweis

Das Menü "I-Features" sowie die zugehörigen Menüpunkte sind nur verfügbar, wenn Sie den SCALANCE W78x im Access Point-Modus verwenden. Die Betriebsart können Sie im Menü "System" festlegen.

Der Menüpunkt iPCF ist nur bei einem SCALANCE W747-1RR, SCALANCE W747-1 und beim IWLAN/PB LINK verfügbar.

5.6.8.2 Menüpunkt iQoS (Nur im Access Point-Modus)

Hinweis

Diese Funktion ist im iPCF-Modus nicht verfügbar.

Clientspezifische Bandbreitenreservierung

iQoS (Quality of Service) ist ein Verfahren, bei dem Clients eine bestimmte Bandbreite zugeordnet bekommen. Aufgrund dieser Zuordnung erfolgt die Datenübertragung zu diesen Clients mit hoher Wahrscheinlichkeit innerhalb eines definierten Zeitraums. Dieses Verfahren kann überall dort sinnvoll eingesetzt werden, wo bestimmte Antwortzeiten gewährleistet werden müssen. Falls Nicht-iQoS-Clients (engl: Non-iQoS Clients) das Netzwerk zu stark belasten, können sie vom AP abgemeldet werden, um den Datenverkehr für iQoS Clients sicher zu stellen.

Hinweis

Um eine einwandfreie Funktion des iQoS-Verfahrens zu gewährleisten, ist die Anzahl der Clients mit Bandbreitenreservierung auf vier begrenzt.

Hinweis

Wenn der Anwender für kritische Clients Daten reserviert, dann beinhaltet diese Datenrate auch die Frame-Header (also z. B. 802.11-, MAC-, IP-, TCP- und S7-Header). Ein SIMATIC-Anwender muss also neben den Netto-Daten auch noch die Header bei seiner Konfiguration berücksichtigen.

Response Time

Im Eingabefeld "Response Time" tragen Sie die gewünschte Antwortzeit des SCALANCE W78x über die Funkschnittstelle ein. Beachten Sie, dass es sich bei diesem Wert um die Übertragungszeit der Daten vom SCALANCE W78x zum Client handelt. Entsprechend dem festgelegten Werte vermindert sich die Datenübertragungsrate für die Netzteilnehmer, die nicht in der Liste aufgeführt sind.

Siehe auch

- Menüpunkt CLI\IFEATURES\IQOS\WLAN1 (bzw. \WLAN2 oder \WLAN3) (Seite 247)

5.6.8.3 Menüpunkt Forced Roaming on IP Down (Nur im Access Point-Modus)

Hinweis

Forced Roaming on IP Down kann nicht zusammen mit iPCF oder WDS auf dem gleichen WLAN-Interface betrieben werden.

Konfiguration

Nach dem Aktivieren des Kontrollkästchens "Forced Roaming on IP Down" können Sie folgende Parameter konfigurieren:

- **Destination IP address**
  Die IP-Adresse des Geräts, für das eine Verbindungsüberwachung stattfinden soll.
- **Interval (100 - 5000 ms)**
  Zyklusdauer in Millisekunden, nach der die IP-Verbindung überprüft wird.
- **Maximum lost packets (1 - 5)**
  Maximale Anzahl der in Folge verlorenen Pakete nach denen die WLAN-Schnittstelle deaktiviert wird.

Siehe auch

- Menüpunkt CLI\IFEATURES\FORCED_ROAM\WLAN1 (bzw. \WLAN2 oder \WLAN3) (Seite 249)

5.6.8.4 Menüpunkt Link Check (Nur im Access Point-Modus)

Hinweis

Diese Funktion ist im iPCF-Modus nicht verfügbar.

Hinweis

Sie können mit der Funktion Link Check nur Verbindungen zu WLAN-Clients überwachen, die Verwendung zusammen mit Redundanz oder WDS ist nicht möglich.

Tabelle der überwachten Geräte

In der Klappliste der Titelzeile "Link Check" legen Sie fest, ob die Verbindungsüberwachung aktiviert (Enabled) oder deaktiviert (Disabled) sein soll. Es werden aber nur die Verbindungen zu solchen Geräten überwacht, bei denen das Optionskästchen in der Spalte "Sel" aktiviert ist.

Sie können Einträge in der Tabelle löschen, indem Sie das entsprechende Optionskästchen in der Spalte "Del" aktivieren und die Schaltfläche "Set Values" anklicken. Neue Listeneinträge legen Sie nach dem Anklicken der Schaltfläche "New" an. Sie können dann die MAC-Adresse und die Überwachungszeit eingeben.

Systemereignis bei Verbindungsabbruch

Wie der SCALANCE W78x auf einen Verbindungsabbruch (oder auch auf das Wiederherstellen einer Verbindung) reagiert, können Sie im Menü **System > Events** festlegen.

Siehe auch

- Menüpunkt CLI\IFEATURES\LINKCHECK (Seite 250)

5.6.8.5 Menüpunkt Redundancy (Nur im Access Point-Modus)

Hinweis

Die hier beschriebene Redundanzfunktion steht nur bei SCALANCE W78x zur Verfügung, die über mehr als eine Funkkarte verfügen und die nicht im iPCF-Modus betrieben werden.

Sie können nur das Verschlüsselungsverfahren **WEP** verwenden.

Konfiguration mit sysName

Anstelle der MAC-Adressen können Sie die redundanten Partner auch mit dem Parameter "sysName" konfigurieren. Beacons enthalten diesen Parameter, deshalb wird das redundante Gerät über Beacons erkannt.

Hinweis

Mit dem FW-Update auf V3.0 ist eine Nachkonfiguration für die Geräte SCALANCE W78x-xRR erforderlich, wenn Sie WDS oder Redundanz nutzen und dabei die MAC-Adresse und nicht die sysNamen benutzen.
Diese Funktionen basieren dann auf der MAC-Adresse, die sich durch die Einführung von VAPs mit der V3.0. ändert.

Hinweis

Wird IEEE 802.1x oder WPA verwendet, muss für die Redundanz-Verbindung ein "Private Key" gewählt werden.

Siehe auch

- Menüpunkt CLI\IFEATURES\REDUNDANCY (Seite 251)

5.6.8.6 Menüpunkt IP Alive (Nur im Access Point-Modus)

Tabelle der überwachten Geräte

In der Klappliste "IP Alive" legen Sie fest, ob die Verbindungsüberwachung aktiviert (Enabled) oder deaktiviert (Disabled) sein soll. Es werden aber nur die Verbindungen zu solchen IP-Adressen überwacht, bei denen das Optionskästchen in der Spalte "Sel" markiert ist.

Sie können Einträge in der Tabelle löschen, indem Sie das entsprechende Optionskästchen in der Spalte "Del" markieren und die Schaltfläche "Set Values" anklicken. Neue Listeneinträge legen Sie nach dem Anklicken der Schaltfläche "New" an. Sie können dann die MAC-Adresse und die Überwachungszeit eingeben.

Überwachung unabhängig vom Port

Bei IP-Alive legen Sie eine Überwachungszeit für eine IP-Adresse und einen Port fest. Falls Sie keinen bestimmten Port, sondern nur den Datenverkehr von einer bestimmten IP-Adresse überwachen wollen, dann tragen Sie beim Port einfach eine 0 ein. Damit wird die Überwachung bei jedem Telegramm von dieser IP-Adresse zurückgesetzt.

Systemereignis bei Verbindungsabbruch

Wie der SCALANCE W78x auf eine Änderung des IP-Alive-Status reagiert, können Sie im Menü **System > Events** festlegen.

Hinweis

Die Funktion IP-Alive ist im iPCF-Modus nicht verfügbar.

Hinweis

Falls die IP Alive-Funktion für die angegebene Zeit keinen Datenverkehr beobachtet, wird der Status für die IP-Adresse auf "Offline" gesetzt und der Fehlerstatus aktiviert. Bevor die IP Alive-Funktion den Status bei aktivem Datenverkehr wieder auf "Online" setzt, muss der Fehlerstatus bestätigt werden.

Siehe auch

- Menüpunkt CLI\IFEATURES\IP_ALIVE (Seite 252)

5.6.9 Das Menü Information

5.6.9.1 Menüpunkt Information

Systemereignisse und Informationen über die Protokolle

Die Seiten dieses Menüs zeigen in tabellarischer Form Informationen zu Systemereignissen und Informationen über das Betriebsverhalten der Protokolle (IP, TCP, UDP, ICMP, SNMP).

Aktualisierung der Anzeige

Die meisten Seiten haben am unteren Rand die Schaltfläche "Refresh" mit der Sie die Anzeige aktualisieren können. Der Menüpunkt "Client List" bietet darüber hinaus die Möglichkeit einer automatischen Aktualisierung. Dazu müssen Sie das Optionskästchen "Update" markieren.

Siehe auch

- Menüpunkt CLI\INFORM (Seite 253)

5.6.9.2 Menüpunkt Log Table

Protokollieren von Systemereignissen

Auf dieser Seite sind Systemereignisse sowie der Zeitpunkt ihres Eintretens aufgeführt. Welche Ereignisse hier vermerkt werden, können Sie im Menü **System > Events** festlegen.

Wenn Sie mit dem Mauszeiger über den Zeitwert gehen, wird die Systemzeit mit Datumsanzeige aufgeblendet.

Siehe auch

- Menüpunkt CLI\INFORM\LOG (Seite 254)

5.6.9.3 Menüpunkt Auth Log

Protokollierung der Authentifizierung

Die Seiten dieses Menüs zeigen in tabellarischer Form Informationen zu erfolgten oder fehlgeschlagenen Authentifizierungsversuchen.

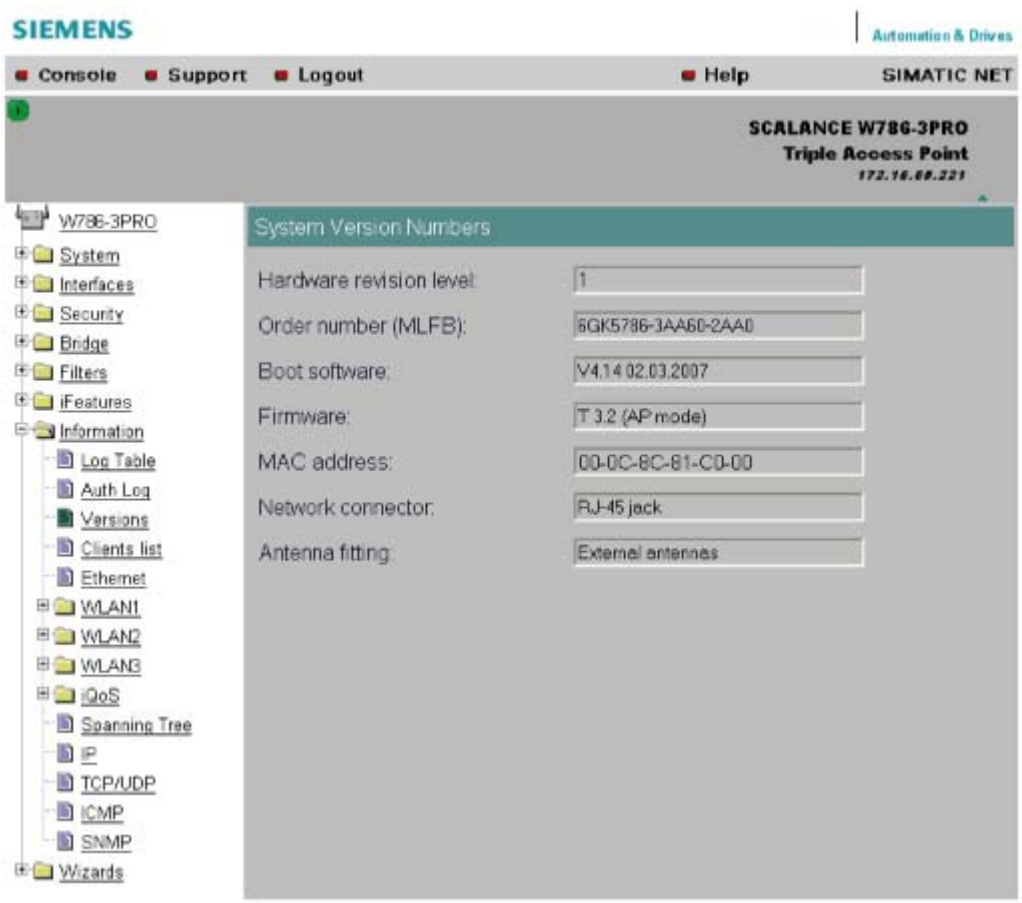
Siehe auch

- Menüpunkt CLI\INFORM\AUTHLOG (Seite 255)

5.6.9.4 Menüpunkt Versions

Aktuelle Versionsstände und Bestellnummern

1. Hardware Ausgabestand
2. Bestellnummer (MLFB)
3. Boot-SW-Version
4. FW-Version
5. Ethernet-MAC-Adresse
6. Typ des Netzwerkanschlusses (RJ-45 elektrisch/ST optisch)
7. Antennenmontage (intern/extern)


SIEMENS
Automation & Drives
Console
Support
Logout
Help
SIMATIC NET
SCALANCE W786-3PRO
Triple Access Point
172.16.88.221
W786-3PRO
System
Interfaces
Security
Bridge
Filters
iFeatures
Information
Log Table
Auth Log
Versions
Clients list
Ethernet
WLAN1
WLAN2
WLAN3
iQoS
Spanning Tree
IP
TCP/UDP
ICMP
SNMP
Wizards
System Version Numbers
Hardware revision level: 1
Order number (MLFB): 6GK5786-3AA60-2AA0
Boot software: V4.14 02.03.2007
Firmware: T 3.2 (AP mode)
MAC address: 00-0C-8C-81-C0-00
Network connector: RJ-45 jack
Antenna fitting: External antennas

5.6.9.5 Menüpunkt Client List

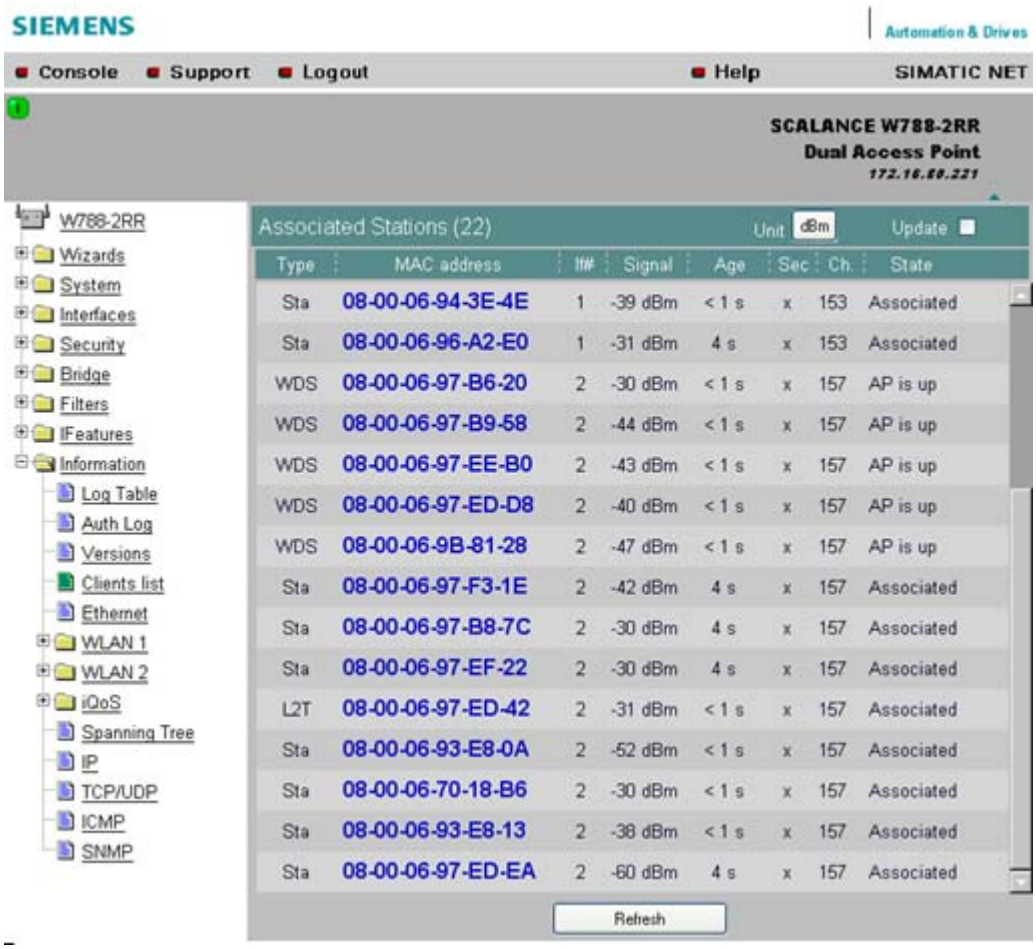
Hinweis

Dieser Menüpunkt ist nur im Access Point-Modus verfügbar.

Angemeldete Clients

Hier werden alle am SCALANCE W78x angemeldeten Clients sowie einige Zusatzinformationen (Funkkanal, Status usw.) angezeigt.

- MAC Address
  Die MAC-Adresse des Clients.
- If#
  Hier ist angegeben, über welche Funkschnittstelle der Client angebunden ist
- Signal
  Die Signalstärke des Clients. Je größer der Wert, desto besser ist das Signal. Der Nutzer kann zwischen Prozent und dBm wählen.
- Age
  Zeigt die vergangene Zeit an, seit dem die letzte Aktivität vom Client erkannt worden ist.
- Sec
  Hier ist angegeben, welche Verschlüsselung aktiviert ist.
- Channel.
  Der aktuelle Kanal, über den der Client mit dem SCALANCE W78x kommuniziert.
- State
  Der aktuelle Zustand der Clients. Associated bedeutet, dass der Client angemeldet ist.



Mit dem Optionskästchen "Update" wird die Liste alle 3 Sekunden automatisch aktualisiert. Wenn Sie auf die MAC-Adresse eines Clients klicken, bekommen Sie weitere Informationen zu diesem Client angezeigt.

Siehe auch

- Menüpunkt CLI\INFORM\WLAN1 (bzw. \WLAN2 oder \WLAN3) (Seite 256)

5.6.9.6 Menüpunkt Ethernet

Informationen über die Ethernet-Schnittstellen

Dieser Menüpunkt liefert Information über die aktuellen Einstellungen der Ethernet-Schnittstelle. Außerdem werden hier die laufenden Betriebsdaten angezeigt.

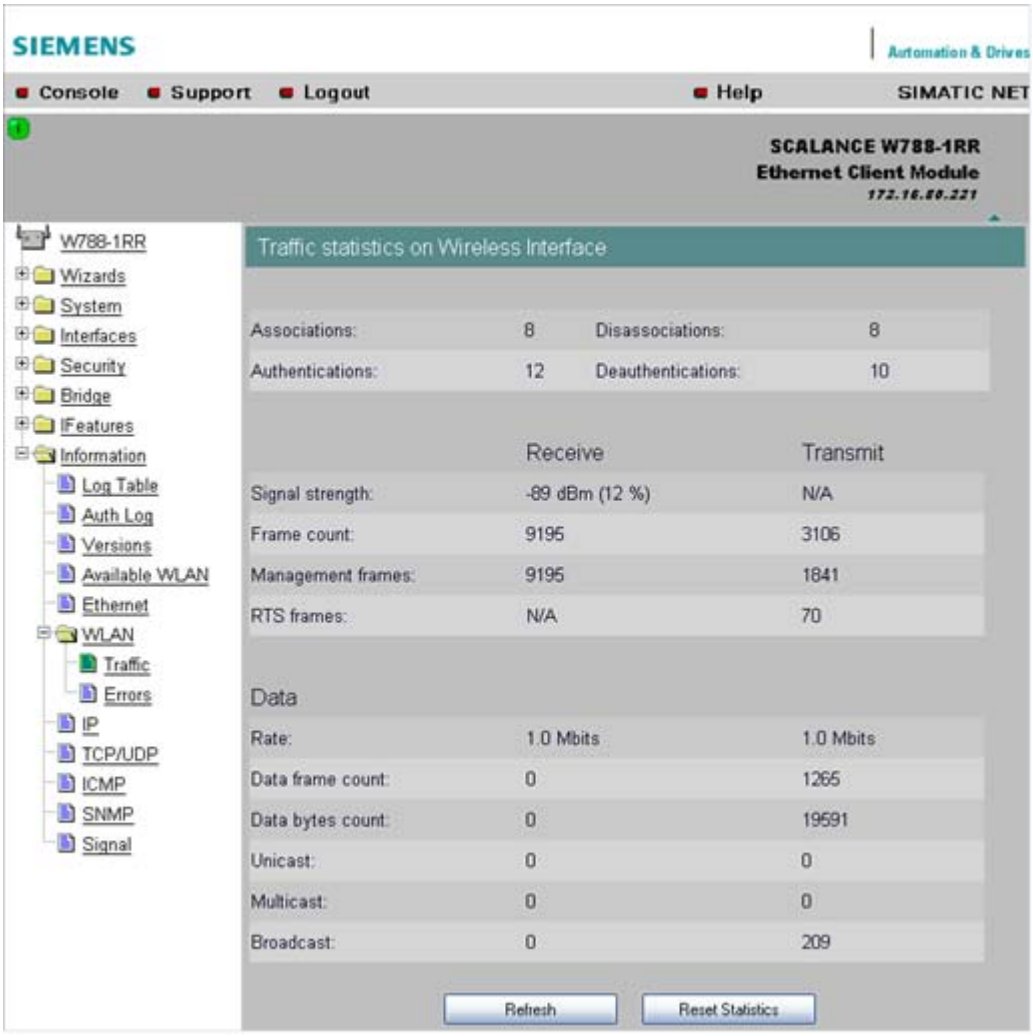
5.6.9.7 Menüpunkt WLAN

Informationen über die WLAN-Schnittstelle

Dieser Menüpunkt liefert Information über die aktuellen Einstellungen der WLAN-Schnittstelle. Außerdem werden hier die laufenden Betriebsdaten angezeigt. Bei den Modellen mit mehr als einer Funkschnittstelle gibt es für jede Funkschnittstelle jeweils einen eigenen Menüpunkt.

Traffic

Hier werden Statistiken für die übertragenen Daten angezeigt.

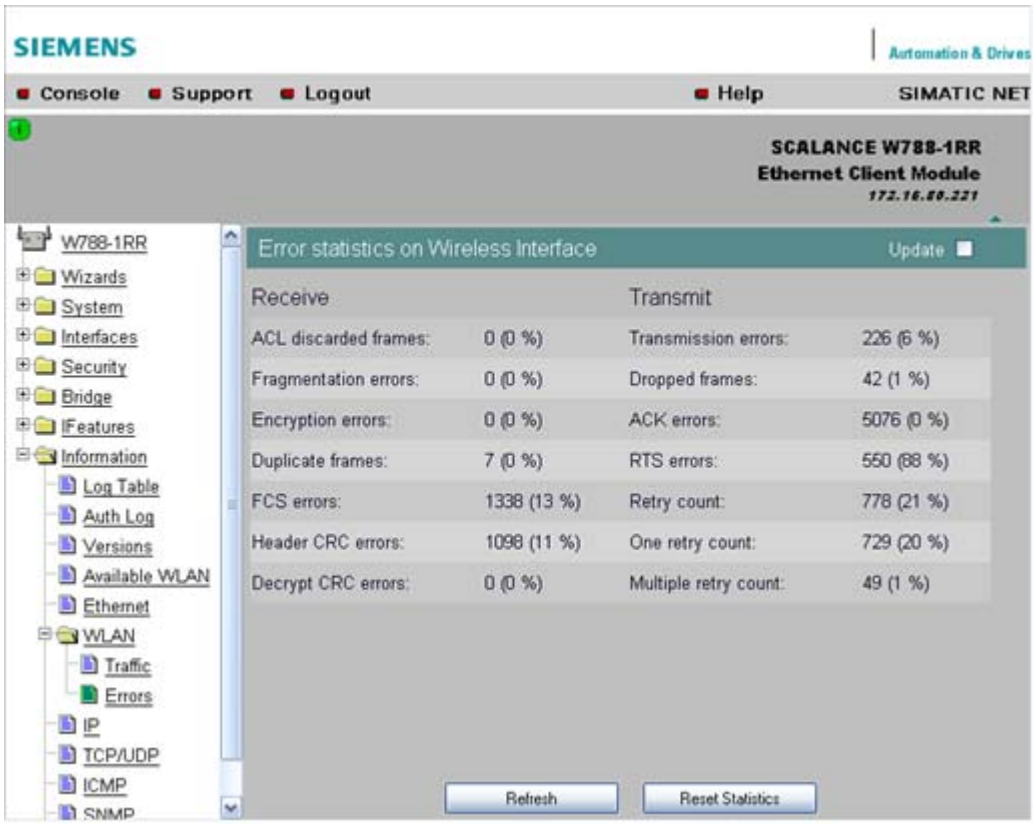


- Association / Authentication Frames
  Gezählt werden die für einen Anmeldevorgang relevanten Telegramme. Es wird unterschieden in den Anmeldetelegrammen Association und Authentication sowie den Abmeldetelegrammen Disassociation und Deauthentication.
- Signal strength
  Angezeigt wird die Signalstärke als Mittelwert der zuletzt empfangenen Telegramme bzw. für die Sendeseite der zuletzt empfangenen Acknowledge Frames.
- Frame count
  Zähler für alle erfolgreich empfangenen oder gesendeten Telegramme.
- Management frames
  Zählt alle empfangenen oder gesendeten Management frames.
- RTS frames
  Wird erhöht wenn auf ein RTS Telegramm ein CTS Telegramm empfangen wird.
- Rate
  Zeigt eine mittlere Datenrate der zuletzt empfangenen oder gesendeten Datenframes an.

- Data frame count
  Zählt alle empfangenen oder gesendeten Datenpakete.
- Data bytes count
  Zeigt die Summe aller empfangenen bzw. gesendeter Bytes in einem Datentelegramm an.
- Unicast
  Summer aller empfangen bzw. gesendeter Daten Unicasts an.
- Multicast
  Summer aller empfangen bzw. gesendeter Daten Multicasts an.
- Broadcast
  Summer aller empfangen bzw. gesendeter Daten Broadcasts an.

Errors

Diese Seite zeigt Statistiken für die aufgetretenen Übertragungsfehlern. Eine hohe Fehleranzahl deutet auf eine schlechte Verbindung hin.



Receive Errors

- ACL discarded frames
  Zeigt alle Anmeldeversuche eines Clients die von der Access Control List geblockt werden.
- Fragmentation errors
  Summe aller gescheiterten Fragmentierungen. Eines der Fragmente wurde nicht oder zu spät empfangen.
- Encryption errors
  Wird erhöht falls ein Telegramm empfangen wird bei dem das WEP Bit gesetzt ist und das Gerät ohne Verschlüsselung arbeitet, bzw. umgekehrt wenn ein Paket ohne WEP Bit gesetzt empfangen wird und Verschlüsselung aktiviert ist.
- Duplicate frames
  Summe aller doppelt empfangener Telegramme.
- FCS errors
  Summe aller empfangener Pakete bei denen die Checksumme falsch war.
- Header CRC error
  Summe aller empfangener Pakete bei denen die Checksumme über das Header falsch war.
- Decrypt CRC error
  Summe aller empfangen Pakete bei denen die Checksumme über den verschlüsselten Datenpuffer falsch war.

Transmit Errors

- Transmission errors
  Wird erhöht wenn ein Telegramm trotz Hardware Retries nicht erfolgreich gesendet werden kann.
- Dropped frames
  Anzahl Pakete die verworfen werden, wenn entweder das Paket trotz aller Retries nicht erfolgreich gesendet worden ist, oder Pakete die noch nicht gesendet worden sind wenn ein Teilnehmer abgemeldet wird.
- Acknowledged errors
  Summe aller gesendeten Pakete die nicht durch ein Acknowledge bestätigt worden sind.
- RTS errors
  Summe aller gesendeten RTS Telegramme die nicht durch ein CTS quittiert worden sind.
- Retry count
  Summe aller erfolgreich gesendeter Telegramme die eine oder mehrere Retries benötigt haben.
- One retry count
  Summe aller erfolgreich gesendeter Telegramme die genau eine Wiederholung benötigt haben.
- Multiple retry count
  Summe aller erfolgreich gesendeter Telegramme die mehr als eine Wiederholung benötigt haben.

Hinweis

Die hinter den Errors stehenden Prozentangaben beziehen sich auf die Gesamtzahl der empfangenen / gesendeten Frames.

Overlap AP

Hinweis

Dieser Menüpunkt ist nur im Access Point-Modus verfügbar.

Für einen optimalen Datendurchsatz ist es notwendig, dass der eingestellte Funkkanal nicht von anderen Access Points genutzt wird. Im 2,4 GHz Band (802.11b oder 802.11g) gibt es eine Überlappung der Funkkanäle, sodass ein Access Point nicht nur den eingestellten Kanal belegt, sondern zusätzlich die benachbarten 2-3 Kanäle. Achten Sie deshalb darauf, dass zu benachbarten Access Points ein ausreichend großer Kanalabstand besteht.

Die Seite "Overlap AP" zeigt alle Access Points, die auf dem eingestellten oder auf benachbarten Kanälen (bei 2,4 GHz) sichtbar sind. Wenn hier Einträge vorhanden sind, ist der maximale Datendurchsatz des Access Points beeinträchtigt.

- Type
  Zeigt die Verbindungsart an. Es gibt die Arten AP (Infrastrukturmodus) und AdHoc.
- MAC address
  Die MAC-Adresse der Funkgeräte.
- Channel
  Der Kanal, auf dem das gefundene Funkgerät sendet.
- Signal
  Zeigt die Signalstärke an, mit der die anderen Funkgeräte beim AP ankommen. Je stärker das Signal desto höher die Wahrscheinlichkeit, dass sie sich untereinander stören. Auch bei geringen Signalstärken besteht die Möglichkeit zur gegenseitigen Beeinflussung.
- Age
  Zeigt an, wann die letzte Aktivität vom Funkgerät erkannt wurde.
- SSID
  Zeigt die SSID des anderen Funkgerätes an.

5.6.9.8 Menüpunkt iQoS

Informationen über die Bandbreitenreservierung

Die Seiten dieses Menüs liefern Informationen über iQoS. Dabei werden die Clients wie folgt eingeteilt:

- Critical Compliant (CC)
  Hierbei handelt es sich um Clients, die als kritisch definiert wurden und die aktuell die von ihnen angeforderte Bandbreite und Antwortzeit einhalten können.
- Critical Non-Compliant (CNC)
  Auch bei den CNC Clients handelt es sich um Clients, die feste Anforderungen an die Antwortzeit und Bandbreite stellen. Im Gegensatz zu den CC Clients gelingt es diesen Clients aktuell nicht, diese Anforderungen einzuhalten.
- Non-Critical Satisfied (NCS)
  Bei diesen Clients handelt es sich um Clients ohne feste Anforderungen an die Antwortzeit/Mindestbandbreite. Sie werden momentan nicht durch iQoS in ihrer Kommunikation eingeschränkt.
- Non-Critical Regulated (NCR)
  Auch hier handelt es sich um unkritische Clients, die aktuell jedoch durch iQoS in ihrer Kommunikation zugunsten kritischer Clients eingeschränkt werden.
- Non-Critical Non-Responsive (NCNR)
  Einige Clients, die für ihre Kommunikation keinerlei Quittierung erfordern (z.B. UDP Verkehr), können durch iQoS nicht geregelt werden. Diese fallen in die Klassifikation NCNR.

Siehe auch

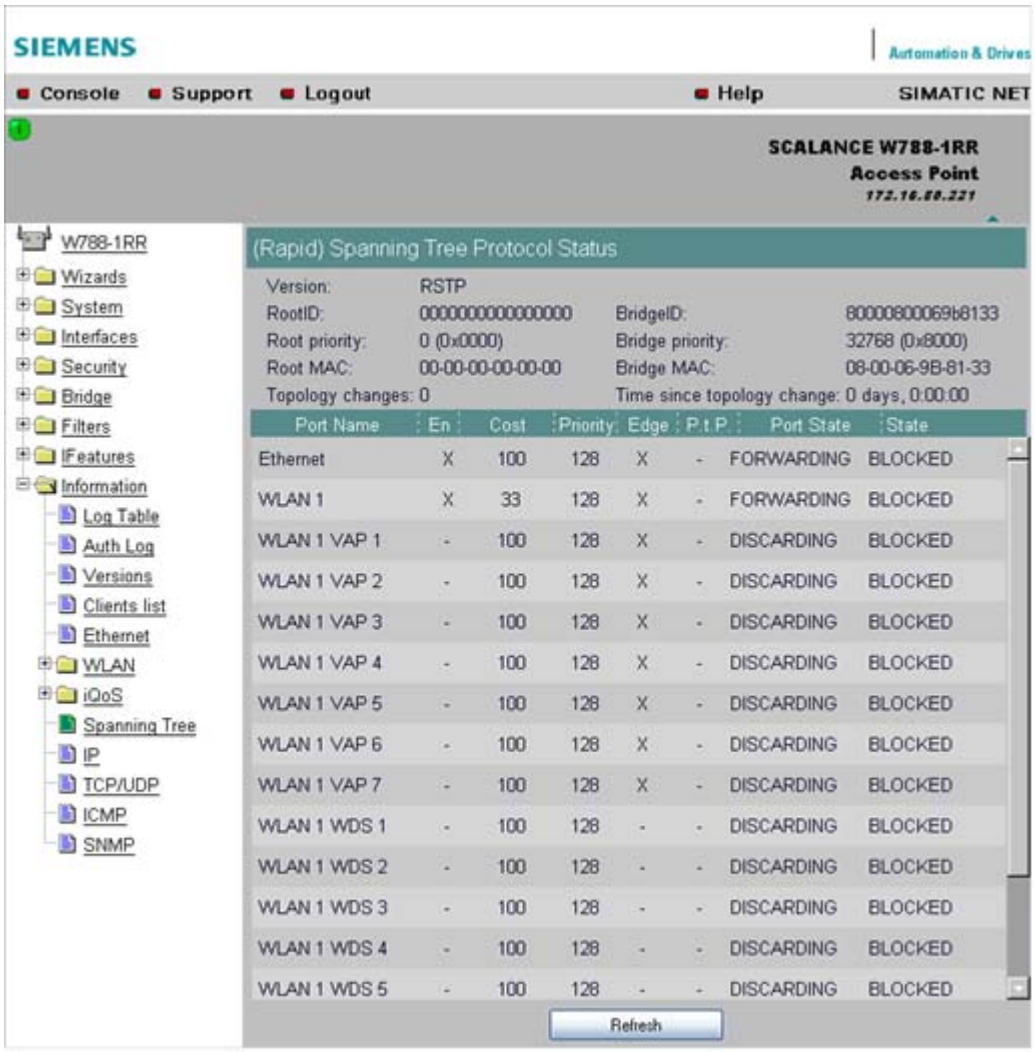
- Menüpunkt CLI\IFEATURES\IQOS\WLAN1 (bzw. \WLAN2 oder \WLAN3) (Seite 247)

5.6.9.9 Menüpunkt Spanning Tree

Status des Spanning Tree-Protokolls

Der obere Teil der Seite zeigt die "RootID" und die "BridgeID". Beide IDs setzen sich aus deren Priorität und deren MAC-Adresse zusammen. Zusammen ergibt das dann die 16 Zeichen lange ID. Die RootID ist die ID der Bridge, die zur Zeit Root-Bridge ist. Die BridgeID zeigt die ID des eigenen Gerätes an.

Darunter sieht man Werte für das Ereignis Topology Change. Der erste Wert ist ein Zähler wie oft sie die Baumstruktur, seit Neustart, geändert hat. Der Wert daneben zeigt die Zeit seit dem letzten Umschaltereignis.



Darunter sind folgende Port-bezogenen Informationen zu finden:

- Port Name
  Klartextname des Ports, z.B. Ethernet oder WLAN1 WDS1.

- Enabled
  Zeigt an, ob das (R)STP für diesen Port aktiviert ist. Ist der Port nicht aktiviert, werden über diesen Port keine Telegramme mehr weitergeleitet.
- Cost
  Zeigt die Pfadkosten für den Port an.
- Priority
  Zeigt die momentane Priorität des Ports an.
- Edge
  Zeigt an ob der Port ein Randpunkt ist oder nicht.
- P.t.P.
  Zeigt an, ob der AP direkt mit einem anderen (R)STP- Gerät verbunden ist
- Port State
  Beim STP kann ein Port drei Zustände annehmen:
  - Discarding
    Es werden keine Telegramme von oder an diesen Port weitergeleitet. Der Port ist vom Anwender oder dem Protokoll (z.B. wenn ein redundanter Weg festgestellt worden ist) deaktiviert worden.
  - Learning
    Der Port empfängt wie im Zustand Listening Pakete, leitet diese aber nicht weiter. Zusätzlich werden die MAC-Adressen in die "Learning Bridge" eingetragen.
  - Forwarding
    Der Port ist komplett freigeschaltet. Er kann Telegramme empfangen und senden.
  - Disabled
    Der Port wird momentan nicht benutzt.
- State
  Hier wird der Zustand des Ports im Bezug auf die Root Bridge angezeigt. Der Zustand "ROOT" bedeutet, das der Port direkt mit der Root Bridge verbunden ist. "DESIGNATED" sind alle Ports, die nicht direkt an der Root liegen, aber freigeschaltet sind. Ports die gesperrt worden sind, befinden sich im Zustand "BLOCKED".

5.6.9.10 Menüpunkt IP, TCP/IP, IPCM, SNMP

Informationen über Protokolle

Die Seiten dieses Menüs zeigen in tabellarischer Form Informationen über die Protokolle IP, TCP, UDP, ICMP und SNMP.

Hinweis

Für diesen Menüpunkt gibt es keine CLI-Befehle.

5.6.9.11 Menüpunkt Signal Recorder

Hinweis

Der Signal Recorder ist nur für Clients und Access Points im Client-Modus sowie für das IWLAN/PB-Link PN IO verfügbar.

Anzeigen der Signalstärke

Mit dem Signal Recorder kann die Signalstärke des verbundenen Accesspoints aufgezeichnet oder angezeigt werden. Mit Hilfe dieser Daten können Sie Gebiete mit unzureichender Signalstärke auffinden. Der Signal Recorder kann besonders dann vorteilhaft eingesetzt werden, wenn sich der Client auf einer fest vorgegebenen Strecke bewegt (z.B. Hängebahn).

- Vorgehensweise bei SCALANCE W-700-Clients:
  Über die URL
  http://<IP-Adresse>/Signal.txt
  als auch über die URL
  http://<IP-Adresse>/Signal.log
  können Sie das erzeugte Signal File herunterladen. Falls Sie noch nicht angemeldet sind, gelangen Sie zum Login Fenster, in dem Sie sich anmelden müssen.
- Vorgehensweise bei IWLAN/PB LINK PNIO:
  1. Aktivieren Sie den FTP-Server
  2. Eingabe in eine DOS-Box `ftp <ip-adresse>`.
  3. Login als admin (Default Passwort admin)
  4. Geben Sie den Befehl get signal.txt ein.
  Die Datei signal.txt wird dann in das Verzeichnis abgelegt, von dem aus der ftp-Befehl (Pkt. 2) erfolgte.

Anzeigen des Momentanwertes

Die obere Hälfte des Teilfensters enthält ein Anzeigeinstrument für die grafische Darstellung des momentan ermittelten dbm-Wertes in Echtzeit. Abhängig von Browser und Netzauslastung wird die Anzeige ca. alle 500 ms aktualisiert. Neben der grafischen Anzeige wird der aktuelle dbm-Wert auch im Klartext dargestellt. Zusätzlich werden die MAC-Adresse

des APs, mit dem das ECM derzeit verbunden ist, sowie Frequenz, Kanal und Senderate dargestellt und entsprechend aktualisiert. Sie können die grafische Anzeige mittels der Schaltflächen "Start display" und "Stop display" starten bzw. stoppen.

Hinweis

Der Betrieb der grafischen Anzeige kann eine nicht unerhebliche Netzlast hervorrufen, die zeit- und durchsatzkritische Prozesse (PNIO) stören kann.

Aufzeichnung einer Messreihe

Die untere Hälfte des Teilfensters enthält neben den Bedienelementen für die grafische Anzeige des Momentanwertes auch die Bedienelemente des eigentlichen Signal Recorders. Sie haben die Möglichkeit das Zeitintervall, welches zwischen der Erfassung zweier Messpunkte liegt, und die Gesamtzahl der Messpunkte, vorzugeben. Der Recorder wird über die Schaltflächen "Start recording" bzw. "Stop recording" gesteuert.

Sobald erfolgreich Messpunkte aufgenommen und der Recorder wieder gestoppt wurde, stehen die Schaltflächen "Save recorder file" und "Display recorder file" zur Verfügung. Die Messwerte können durch betätigen der "Save"-Schaltfläche als Datei im CSV-Format direkt vom ECM geladen und in ein geeignetes Auswerteprogramm importiert werden.

Die CSV-Datei enthält für jeden Messpunkt die MAC-Adresse des APs, die laufende Nummer der Messung, den Rohwert der RSSI, den dBm-Wert und die prozentuale Entsprechung, einen Roaming-Indikator, den Kanal und die Senderate.

Die "Display record file" -Schaltfläche öffnet ein Pop-Up Fenster, in dem der Verlauf der Messwerte bereits grafisch aufbereitet vorliegt. Dargestellt wird der Verlauf der dBm-Werte. Roamt das ECM während der Messung, weisen blaue Balken auf das Ereignis hin. Bewegt man den Mauszeiger auf einen solchen Balken bzw. auf das Fähnchen oben am Balken, so erscheint ein Tooltip mit den MAC-Adressen der beiden Accesspoints.

Mit der Schaltfläche "Print graph" ist es möglich die Tabelle auf einfache Weise auszudrucken, hierzu müssen jedoch im Browser Einstellungen vorgenommen werden.

- Mozilla Firefox 1.5:
  Im Dialog "Datei" => "Seite einrichten..." muß im Feld "Optionen" für Hintergrund drucken (Farben und Bilder) ein Häkchen gesetzt werden.
- Microsoft Internet Explorer 6.0:
  Unter "Extras" => "Internetoptionen" => "Erweitert" muss unter dem Eintrag "Drucken" bei Hintergrundfarben und -bilder drucken ein Häckchen gesetzt werden.

Der Signal Recorder selber verursacht keine nennenswerte Netzlast, die andere Prozesse beeinträchtigen könnte.

Beide Teile des Signal Recorders lassen sich unabhängig voneinander betreiben.

Hier einige Anwendungshinweise, um aussagekräftige Messungen mit dem Signalrekorder zu erhalten:

- Benutzen Sie bei der Konfiguration eine fixe Datenrate.
- wenn möglich sollte für die Messungen der Betriebsmodus ipcf mit möglichst geringer Aktualisierungszeit eingestellt werden.
- es muss sichergestellt werden, dass genügend Datenkommunikation während der Messung besteht, weil die Statistik die ankommenden Telegramme auswertet.

- die Messstrecke sollte 2-3 Mal mit den gleichen Parametern abgefahren werden, um herauszufinden, ob Einschnitte in der Signalstärke immer an der gleichen Position vorkommen.
- Punktuell sollten Messungen in einer festen Position über eine bestimmte Zeit aufgenommen werden.

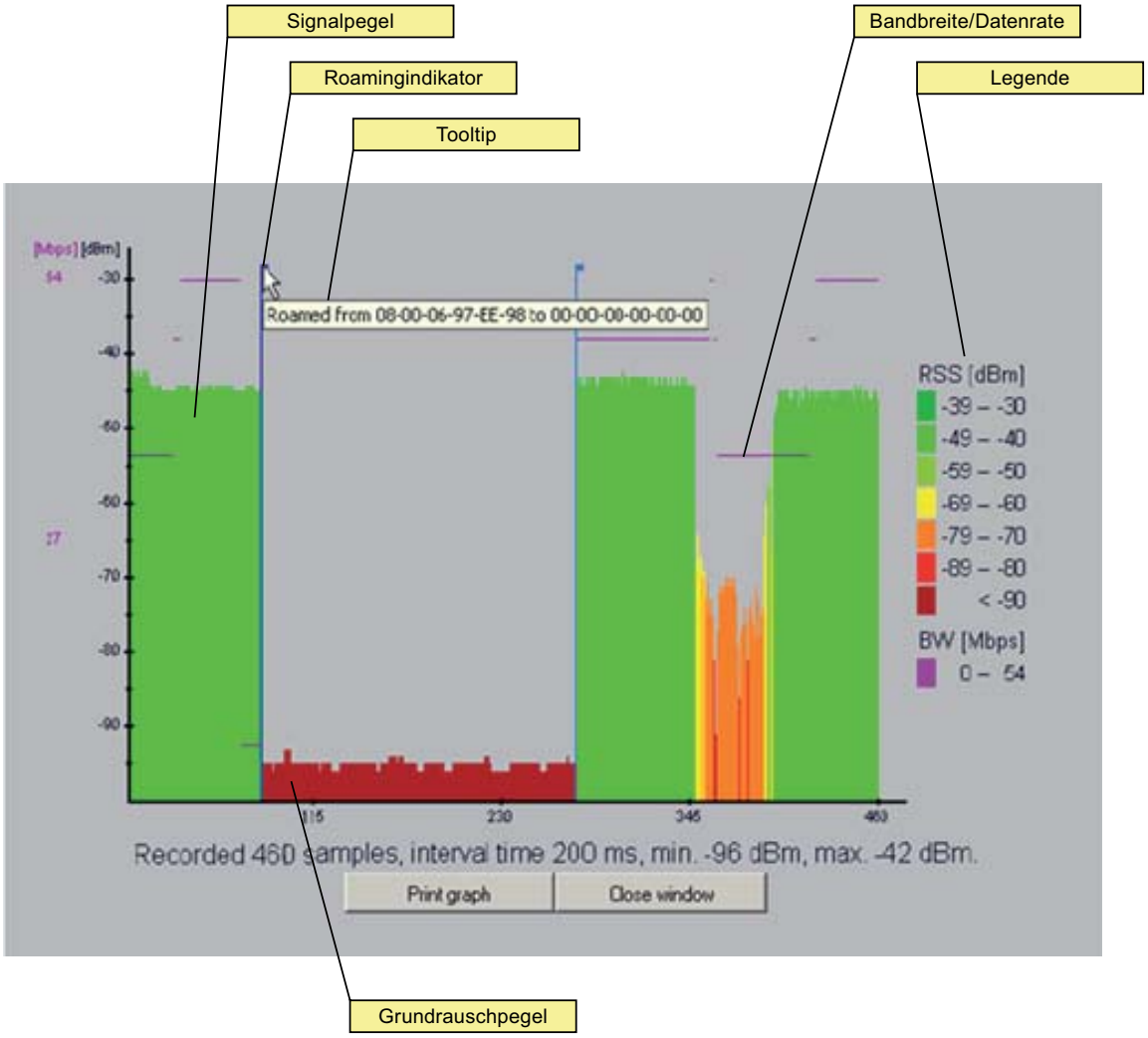


Bild 5-2 Bildschirmdarstellung der Messwerte

Roamingindikator
Dieser Wert erscheint, wenn sich der Client auf einen (anderen) bzw. keinen AP verbindet, sich somit die MAC Adresse des APs ändert.

Bandbreite/Datenrate
Die Bandbreite/Datenrate wird nicht durchgezogen dargestellt, da es unter ungünstigen. Bedingungen zu Überdeckungen mit dem Signalpegel kommen kann.

Grundrauschpegel (noise floor)
Das Grundrauschen stellt das untere Ende des technischen Übertragungsbereichs des Gerätes dar. Das bedeutet, dass ab Überschreiten des Grundrauschpegels (das Nutzsignal

wird lauter als das Grundgeräusch) die Systemdynamik beginnt. Aus diesem Grund ist dieser Pegel ist nur dann sichtbar, wenn der Client keine Verbindung zu einem AP hat (im Bild oben durch die MAC Adresse 00-00-00-00-00-00 angedeutet).

Legende
BW Bandwidth in Mbps
RSS Received Signal Strength in dBm

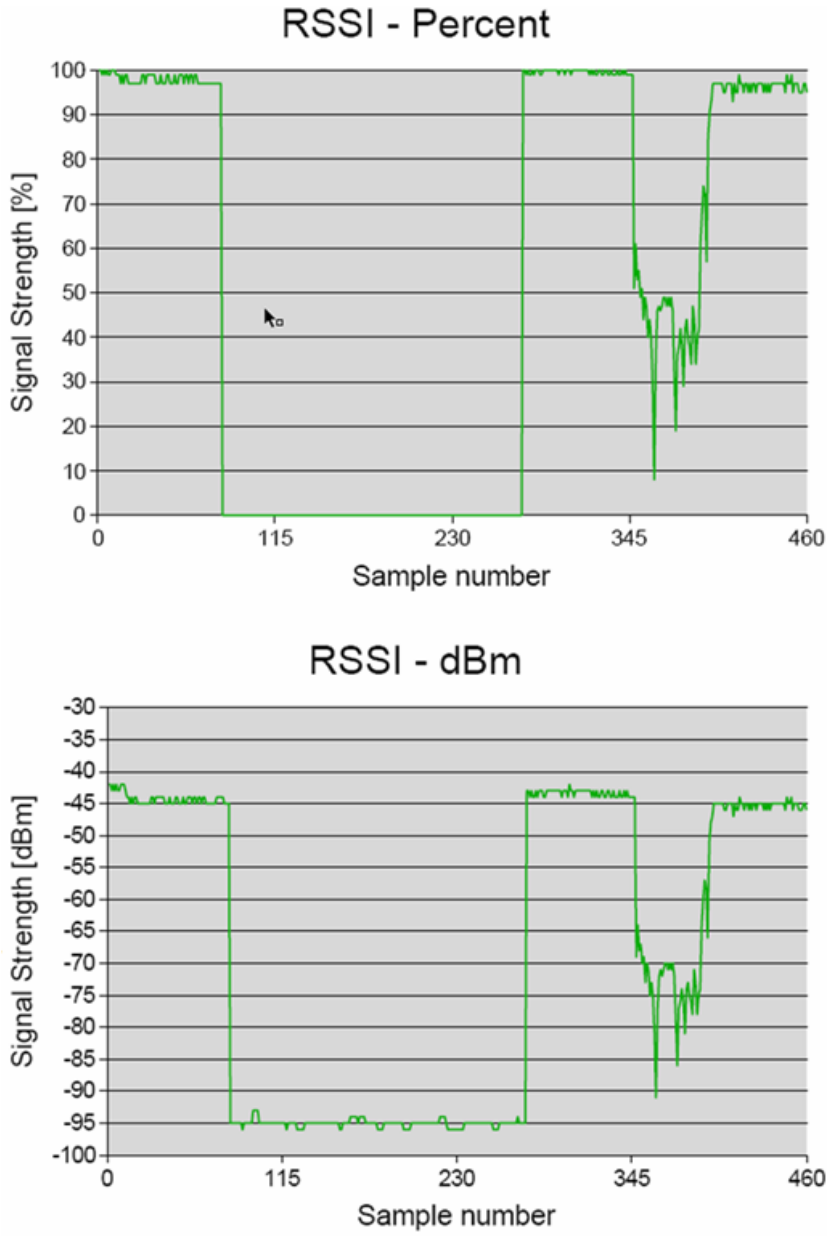


Bild 5-3 Gegenüberstellung der Messwertdarstellung in Prozent und dBm

Siehe auch

- Menüpunkt CLI\INFORM\SIGNAL (Seite 257)

5.7 Konfiguration mit dem Command Line Interface

5.7.1 Allgemeine Informationen über das Command Line Interface

Einleitung

Mit dem Command Line Interface (abgekürzt CLI) können alle Einstellungen eines SCALANCE W-700 und eines IWLAN/PB-Link konfiguriert werden. Das CLI bietet also die gleichen Möglichkeiten wie das Web Based Management. Beachten Sie deshalb auch die ausführlichen Erklärungen zu den Parametern im Kapitel "Konfiguration über das Web Based Management".

Mit dem CLI ist auch eine Remote-Konfiguration über Telnet möglich.

Hinweis

Sie sollten das Command Line Interface nur benutzen, wenn Sie ein erfahrener Benutzer sind. Auch Befehle, die eine grundlegende Änderung der Konfiguration bewirken, werden meistens ohne Rückfrage ausgeführt.

Konfiguration eines IWLAN/PB-Link mit dem CLI

Der IWLAN/PB LINK nutzt ausschließlich die Konfiguration über CLI. In den nachfolgenden Tabellen ist in der Spalte "Kommentar" angegeben, für welches Gerät der entsprechende Befehl verfügbar ist.

Starten des CLI in einer Windows-Konsole

Führen Sie folgende Schritte aus, um das Command Line Interface in einer Windows-Konsole aufzurufen:

1. Öffnen Sie eine Windows-Konsole und geben Sie den Befehl "telnet" gefolgt von der IP-Adresse des SCALANCE W7xx ein:

   ```
   C:\>telnet <IP-Adresse>
   ```

2. Geben Sie Ihr Login und Ihr Passwort ein.

   Alternativ dazu können Sie auch im Menü **Start > Ausführen** den Befehl "telnet" gefolgt von der IP-Adresse des SCALANCE W-700 eingeben.

Starten des CLI über das Web Based Management

Sie können das CLI auch aus dem Web Based Management aufrufen. Klicken Sie auf den Eintrag Console in der oberen Menüleiste des Web Based Managements. Es öffnet sich ein Konsolen-Fenster, in dem Sie sich mit Ihrem Login und Passwort anmelden können. Die IP-Adresse wird vom Web Based Management übernommen.

Hinweis

Diese Funktion ist beim Internet Explorer ab Version 7 nicht verfügbar.

Verkürzte Befehlseingabe

Alternativ zur vollständigen Eingabe von CLI-Befehlen können Sie den/die ersten Buchstaben des Befehls eingeben und dann die Tabulator-Taste drücken. Das Command Line Interface zeigt dann einen Befehl an, der mit dem/den eingegebenen Buchstaben anfängt. Wenn nicht der gewünschte Befehl angezeigt wird, drücken Sie erneut die Tabulator-Taste, um den nächsten Befehl anzuzeigen.

Verzeichnisstruktur

Bevor Sie im Command Line Interface einen bestimmten Befehl eingeben können, müssen Sie erst das entsprechende Menü oder Untermenü aufrufen. In den folgenden Tabellen sind die Befehle eines Menüs sowie mit ihrer Beschreibung wiedergegeben. Das Menü, das die Befehle enthält, ist der Tabelle vorangestellt. In der Tabelle sind nur die Befehle selbst aufgeführt.

Symbolik für die Darstellung der CLI-Befehle

CLI-Befehle haben in der Regel einen oder mehrere Parameter, die in der Syntaxbeschreibung wie folgt dargestellt werden:

- Notwendige Parameter sind durch spitze Klammern gekennzeichnet.
  Beispiel: `<IP-Adresse>`
- Optionale Parameter sind durch eckige Klammern gekennzeichnet.
  Beispiel: `[E|D]`
  Wenn Sie einen optionalen Parameter weglassen, geben die Befehle den aktuell gesetzten Wert aus.
- Alternative Eingabewerte sind durch einen senkrechten Strich getrennt. Sie müssen dann **einen** der aufgeführten Werte als Parameter angeben.
  Beispiel: `[E|D]`
  Sie müssen entweder "E" oder "D" eingeben.
- Wenn Sie als notwendiger Parameter einen Zahlenwert eingeben müssen, kann auch ein Wertebereich angegeben sein:
  Beispiel: `<0 ... 255>`
  Sie müssen einen Wert zwischen 0 und 255 eingeben.

Menüunabhängige Befehle

Die Befehle in der folgenden Tabelle können Sie in jedem Menü aufrufen.

CLI\ ... >

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
/	Wechselt eine Menüebene nach oben.	✔	✔	✔	✔	✔	✔
?	Zeigt die im jeweiligen Menü verfügbaren Befehle und Untermenüs an.	✔	✔	✔	✔	✔	✔
exit	Beendet die CLI/Telnet-Sitzung.	Nicht über die verkürzte Befehlseingabe aufrufbar.					
		✔	✔	✔	✔	✔	✔
restart	Neustart des SCALANCE W7xx	Nicht über die verkürzte Befehlseingabe aufrufbar.					
		✔	✔	✔	✔	✔	✔
info	Zeigt Informationen zum jeweiligen Menüpunkt an.	✔	✔	✔	✔	✔	✔

5.7.2 Das Menü CLI\SYSTEM

5.7.2.1 Menüpunkt CLI\SYSTEM

Betriebsart und Ländereinstellung

Mit den Befehlen dieses Menüs legen Sie die Länderkennung und die Betriebsart (Access Point oder Client) fest.

CLI\SYSTEM>

Befehl	Beschreibung		Kommentar					
			IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`apmode [E|D|H]`	E	Access Point	—	—	—	—	✔	✔
	D	Client						
	H	HiPath Access Point (nur bei SCALANCE W788-2RR verfügbar)						
`country [xx|?]`	Legt fest, welche länderspezifischen Eigenschaften verfügbar sind. Die Ländercodes ("xx") entsprechen ISO 3166. Welche Länder Sie einstellen können, wird nach Eingabe des Befehls "country ?" angezeigt. Es erscheint eine Liste der Länder mit dem zugehörigen zweistelligen Code.		Bei der Ausführung für USA ist dieser Befehl nicht vorhanden.					
			✔	✔	✔	✔	✔	✔
`name [Systemname]`	Ordnet der MIB-Variablen *sysName* einen Wert zu.		Maximal 255 Zeichen. Falls Sie den Namen in WDS oder Redundanz benutzen wollen, dann beträgt die maximale Länge 32 Zeichen.					
			✔	✔	✔	✔	✔	✔
`location [Standort]`	Ordnet der MIB-Variablen *sysLocation* einen Wert zu.		Maximal 255 Zeichen.					
			✔	✔	✔	✔	✔	✔
`contact [Name]`	Ordnet der MIB-Variablen *sysContact* einen Wert zu.		Maximal 255 Zeichen.					
			✔	✔	✔	✔	✔	✔
`ping [-c n | -s] <IP|Name>`	Für Verbindungstest zum Partner. -c (counter) für die Anzahl n der ICMPs -s stoppt den Verbindungstest für alle Geräte		Nur Telnet					
			✔	✔	✔	✔	✔	✔
`password [admin|user] [Passwort]`	Legt ein Passwort für den Zugang zum Gerät fest.		Maximal 31 Zeichen.					
			✔	✔	✔	✔	✔	✔

5.7.2.2 Menüpunkt CLI\SYSTEM\IP

Zuweisung IP-Adresse

Mit den Befehlen dieses Menüs legen Sie fest, wie das Gerät seine IP-Adresse erhält.

CLI\SYSTEM\IP>

Befehl	Beschreibung		Kommentar					
			IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`dhcp [E|D]`	DHCP-Server aktivieren / deaktivieren.		—	✔	✔	✔	✔	✔
`dhcptype [M|N|C]`	Legt fest, wie ein Gerät identifiziert werden soll:		—	✔	✔	✔	✔	✔
	M	MAC-Adresse						
	N	Gerätename						
	C	Client-ID						
`clientid`	Legt eine Client-ID für das Gerät fest.		—	✔	✔	✔	✔	✔
`ip [IP-Adresse]`	Festlegen der IP-Adresse für den SCALANCE W7xx.		Beim Eingeben einer gültigen IP-Adresse wird aktiviertes DHCP automatisch deaktiviert.					
			—	✔	✔	✔	✔	✔
`subnet [Subnetzmaske]`	Festlegen der Subnetzmaske.		—	✔	✔	✔	✔	✔
`gateway [IP-Adresse]`	Festlegen der IP-Adresse des Routers.		—	✔	✔	✔	✔	✔
`ttl [TTL-Wert]`	Setzen des Parameters TTL (Time To Live).		Defaultwert: 64					
			—	✔	✔	✔	✔	✔

Siehe auch

- Menüpunkt IP Einstellungen (Seite 109)

5.7.2.3 Menüpunkt CLI\SYSTEM\SERVICES

Konfigurationsmöglichkeiten

Mit den Befehlen dieses Menüs wählen Sie aus, über welche Dienste (SNMP, Web Based Management usw.) ein Zugriff auf das Gerät möglich sein soll.

CLI\SYSTEM\SERVICES>

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`telnet [E|D]`	Konfiguration des Geräts über Telnet aktivieren / deaktivieren.	Nur WEB und SNMP					
		✔	✔	✔	✔	✔	✔
`ttimeout [E|D]`	Aktiviert / deaktiviert die Zeitbeschränkung für eine Telnet-Sitzung.	✔	✔	✔	✔	✔	✔
`ttimeout [Zeit in s]`	Legt die Zeitdauer fest, nach der eine Telnetsitzung beendet wird, wenn keine Eingabe mehr erfolgt.	✔	✔	✔	✔	✔	✔
`ssh [E|D]`	Aktiviert / deaktiviert die Konfiguration des Gerätes über Sicheres Telnet.	✔	✔	✔	✔	✔	✔
`snmp [E|D]`	SNMP aktivieren / deaktivieren.	—	✔	✔	✔	✔	✔
`mail [E|D]`	E-Mail aktivieren / deaktivieren.	—	✔	✔	✔	✔	✔
`web [E|D]`	Konfiguration des Geräts über Web Based Management aktivieren / deaktivieren.	—	✔	✔	✔	✔	✔
`httpsonly [E|D]`	Zugriff zum Konfigurieren nur über HTTPS aktivieren / deaktivieren.	—	✔	✔	✔	✔	✔
`ping [E|D]`	Antworten des Gerätes auf Ping aktivieren / deaktivieren.	✔	✔	✔	✔	✔	✔
`psu [E|D]`	Zugriff auf das Gerät mit dem Primary Setup Tool aktivieren / deaktivieren. Wenn diese Zugriffsmöglichkeit deaktiviert ist, können die Konfigurationsdaten mit dem Primary Setup Tool nur gelesen werden.	—	✔	✔	✔	✔	✔
`ftpserv [E|D]`	FTP-Server auf dem Gerät aktivieren/deaktivieren. Wird zum Herunterladen der Signal.TXT Datei benötigt, die mit Signal-Recorder erzeugt wurde.	✔	—	—	—	—	—

Siehe auch

- Menüpunkt Services (Seite 109)

5.7.2.4 Menüpunkt CLI\SYSTEM\RESTARTS

Defaulteinstellungen und Neustart

Mit den Befehlen dieses Menüs können Sie Werkseinstellungen des Geräts wiederherstellen und das Gerät neu starten.

CLI\SYSTEM\RESTARTS>

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`restart`	Neustart des Geräts.	Dieser Befehl kann aus allen Menüs aufgerufen werden, allerdings nicht über die verkürzte Befehlseingabe.					
		✔	✔	✔	✔	✔	✔
`memreset`	Wiederherstellen der Werkseinstellungen und Neustart (die geschützten Einstellungen werden nicht gelöscht).	Führen Sie nach dem Wiederherstellen der Werkseinstellungen einen Neustart manuell durch.					
		✔	✔	✔	✔	✔	✔
`defaults`	Wiederherstellen der Werkseinstellungen (auch die geschützten Einstellungen werden gelöscht).	✔	✔	✔	✔	✔	✔

Siehe auch

- Menüpunkt Restart (Seite 110)

5.7.2.5 Menüpunkt CLI\SYSTEM\EVENT

Syntax Command Line Interface

Für jede der vier möglichen Reaktionen EMail, Trap, Log und Fault wird entweder "E" (Enabled, Einstellung ist aktiviert) oder "D" (Disabled = Einstellung ist deaktiviert) als Parameter eingetragen. Soll beispielsweise beim Neustart des Geräts (erster Parameter "CW") eine EMail versendet werden und ein Eintrag in die Log-Tabelle erfolgen aber weder ein Trap noch ein Fehler erzeugt werden, muss folgender Befehl eingegeben werden:

`setec CW E D E D` (für SCALANCE W-700)

`setec CW D E D` (für IWLAN/PB LINK)

Hinweis

Der IWLAN/PB LINK unterstützt keine E-Mail. Dadurch entfällt der zweite Parameter zum aktivieren/deaktivieren der E-Mail Option.

CLI\SYSTEM\EVENT>

Befehle, die nur für Access Points und Client-Module verfügbar sind (nicht für IWLAN/PB LINK):

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`setec CW <E|D> <E|D> <E|D> <E|D>`	Reaktionen beim Neustart des SCALANCE W-700.	—	✔	✔	✔	✔	✔
`setec LU <E|D> <E|D> <E|D>`	Reaktion auf das Ereignis "Link UP" an der Ethernet-Schnittstelle.	Falls der Fehler-Status nur wegen eines Link Down-Ereignisses ausgelöst wurde, wird der Fehlerzustand gelöscht und die Fehler LED erlischt.					
		—	✔	✔	✔	✔	✔
`setec LD <E|D> <E|D> <E|D>`	Reaktion auf das Ereignis Link Down an der Ethernet-Schnittstelle.	—	✔	✔	✔	✔	✔
`setec AF <E|D> <E|D> <E|D>`	Reaktion auf eine fehlerhafte Authentifizierung über das Web Based Management, CLI oder SNMP.	Die SNMP-Trap "AuthFault" wird nur im Falle einer fehlerhafte SNMP-Authentifizierung versendet.					
		—	✔	✔	✔	✔	✔
`setec PM <E|D> <E|D> <E|D> <E|D>`	Reaktion auf einen Wechsel der Spannungsversorgung über M12 Spannungsverbindung.	—	✔	✔	✔	✔	✔
`setec PE <E|D> <E|D> <E|D> <E|D>`	Reaktion auf einen Wechsel der Spannungsversorgung über Ethernet.	—	✔	✔	✔	✔	✔
`setec FC <E|D> <E|D> <E|D>`	Reaktion auf eine Änderung des Fehlerstatus.	—	✔	✔	✔	✔	✔

Befehle, die nur für Access Points verfügbar sind (nicht für Access Points im Client-Modus, Clients, IWLAN/PB LINK):

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`setec AP <E|D> <E|D> <E|D> <E|D>`	Reaktion beim Erkennen eines Access Points auf dem eigenen oder einem überlappenden Funkkanal.	—	—	—	—	✔	✔
`setec MS <E|D> <E|D> <E|D> <E|D>`	Reaktion, wenn durch einen zusätzlichen Client die Updatezeit im iPCF-Modus mit PNIO-Support nicht eingehalten werden kann.	Dieser Befehl ist nur bei folgenden Modellen verfügbar: • SCALANCE W788-1RR • SCALANCE W788-2RR • SCALANCE W784-1RR					
		—	—	—	—	—	✔
`setec CT <E|D> <E|D> <E|D> <E|D>`	Reaktion, wenn die angegeben Update Time im iPCF-Modus mit PNIO-Support nicht eingehalten werden kann.	Dieser Befehl ist nur bei folgenden Modellen verfügbar: • SCALANCE W788-1RR • SCALANCE W788-2RR • SCALANCE W784-1RR					
		—	—	—	—	—	✔
`setec IS <E|D> <E|D> <E|D> <E|D>`	Reaktion auf eine Änderung des Verbindungszustandes bei einem Client, für den die IP-Alive-Überwachung aktiv ist.	Falls sich der Verbindungszustand ändert, wird ein Ereignis ausgelöst. Falls keine Verbindung mehr besteht, wird der Fehlerzustand ausgelöst und die Fehler-LED leuchtet.					
		—	—	—	—	✔	✔
`setec LI <E|D> <E|D> <E|D> <E|D>`	Reaktion bei der Aufnahme einer Verbindung, die durch die Funktion *Link Check* überwacht wird.	—	—	—	—	✔	✔
`setec IQ <E|D> <E|D> <E|D> <E|D>`	Reaktion auf eine Änderung des iQoS-Status.	—	—	—	—	✔	✔
`setec RD <E|D> <E|D> <E|D> <E|D>`	Reaktion auf eine Änderung des Redundancy Event Status.	—	—	—	—	✔	✔
`setec CA <E|D> <E|D> <E|D>`	Reaktion beim Anmelden eines Client.	—	—	—	—	✔	✔
`setec CD <E|D> <E|D> <E|D>`	Reaktion beim Abmelden eines Client.	—	—	—	—	✔	✔
`setec FR <E|D> <E|D> <E|D>`	Reaktion auf die Funktion von Forced Roaming on IP down.	—	—	—	—	✔	✔
`setec ST <E|D> <E|D> <E|D>`	Reaktion bei einer Topologie-Änderung von (Rapid) Spanning Tree.	—	—	—	—	✔	✔
`setec WD <E|D> <E|D> <E|D>`	Reaktion auf den Verbindungsstatus von WDS.	—	—	—	—	✔	✔

		Kommentar					
`setec CP <E|D> <E|D> <E|D>`	Reaktion, wenn die Zykluszeit im iPCF-Modus mit PNIO-Support nicht eingehalten werden konnte.	—	—	—	—	✔	✔

Befehle, die nur für den IWLAN/PB LINK verfügbar sind (nicht für Access Points und Clients):

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`setec CW <E|D> <E|D> <E|D>`	Reaktionen beim Neustart des IWLAN/PB LINK	✔	—	—	—	—	—
`setec P1 <E|D> <E|D> <E|D>`	Reaktion auf einen Wechsel der Spannungsversorgung über die Spannungsverbindung 1.	✔	—	—	—	—	—
`setec P2 <E|D> <E|D> <E|D>`	Reaktion auf einen Wechsel der Spannungsversorgung über die Spannungsverbindung 2.	✔	—	—	—	—	—
`setec FC <E|D> <E|D>`	Reaktion auf eine Änderung des Fehlerstatus.	✔	—	—	—	—	—

5.7.2.6 Menüpunkt CLI\SYSTEM\EMAIL

Absender und Empfänger einer E-Mail

Mit den Befehlen dieses Menüs legen Sie fest, an der das Gerät bei bestimmten Ereignissen eine E-Mail sendet. Außerdem können Sie eine Absenderadresse festlegen.

CLI\SYSTEM\EMAIL

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`mail [E|D]`	Aktivieren / deaktivieren des E-Mail Dienstes.	—	✔	✔	✔	✔	✔
`email [EMail-Adresse]`	Legt fest, an welche Adresse(n) der SCALANCE W-700 E-Mail(s) versendet.	Mehrere E-Mail-Adressen können durch Semikolons getrennt eingegeben werden.					
		—	✔	✔	✔	✔	✔
`smtp <IP-Adresse> [:Port-Nummer]`	Legt die IP-Adresse und Port-Nummer des SMTP-Servers fest.	—	✔	✔	✔	✔	✔
`from [Text für Absenderfeld]`	Legt den Absender für E-Mails vom SCALANCE W-700 fest.	—	✔	✔	✔	✔	✔

Siehe auch

- Menüpunkt E-Mail Config (Seite 113)

5.7.2.7 Menüpunkt CLI\SYSTEM\SNMP

Aktivieren von SNMP

Mit den Befehlen dieses Menüs konfigurieren Sie allgemeine SNMP-Parameter (Aktivieren von SNMP, Traps und Community Strings)

CLI\SYSTEM\SNMP>

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`snmp [E|D]`	Aktiviert / deaktiviert SNMP.	Aktiviert / deaktiviert SNMPv1, v2c, v3 und Traps.					
		—	✔	✔	✔	✔	✔
`snmpv1 [E|D]`	Aktiviert / deaktiviert SNMPv1/v2c.	Aktiviert / deaktiviert SNMPv1, v2c und Traps.					
		—	✔	✔	✔	✔	✔
`snmpv3 [E|D]`	Aktiviert / deaktiviert SNMPv3.	Die besonderen Eigenschaften von SNMPv3 werden erst wirksam, wenn Sie SNMPv1 deaktivieren. Das Aktivieren von SNMPv3 deaktiviert SNMPv1 nicht automatisch.					
		—	✔	✔	✔	✔	✔
`snmpro [E|D]`	Aktiviert / deaktiviert SNMPv1/v2c read only.	—	✔	✔	✔	✔	✔
`getcomm [Read community string]`	Legt den Read community string fest, maximale Länge 63 Zeichen	Defaultwert ist "public".					
		—	✔	✔	✔	✔	✔
`setcomm [Write community string]`	Legt den Write community string fest, maximale Länge 63 Zeichen.	Defaultwert ist "private".					
		—	✔	✔	✔	✔	✔
`trapcomm [Trap community string]`	Legt den Trap community string fest, maximale Länge 63 Zeichen.	Defaultwert ist "public".					
		—	✔	✔	✔	—	—
`traps [E|D]`	Aktiviert / deaktiviert SNMPv1 Traps	Traps sind dann aktiviert, falls SNMP v1, v2c auch aktiviert ist.					
		—	✔	✔	✔	✔	✔

Siehe auch

- Menüpunkt SNMP Config (Seite 113)

5.7.2.8 Menüpunkt CLI\SYSTEM\SNMP\GROUP

SNMP-Gruppen verwalten

Mit den Befehlen dieses Menüs verwalten Sie SNMP-Gruppen (Anlegen, Löschen usw.).

CLI\SYSTEM\SNMP\GROUP>

Befehl	Beschreibung		Kommentar					
			IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`add <Name> [NOAUTH|AUTH|PRIV] [R|W]`	Fügt eine SNMPv3 Gruppe mit folgenden Sicherheitseinstellungen ein		Schreibzugriff ohne Lesezugriff ist nicht möglich.					
			—	✔	✔	✔	✔	✔
	NOAUTH	Keine Authentifizierung, keine Verschlüsselung						
	AUTH	Authentifizierung mit MD5 oder SHA Algorithmus, keine Verschlüsselung						
	PRIV	Authentifizierung mit MD5 oder SHA Algorithmus, und Verschlüsselung mit DES3 Algorithmus						
	Außerdem kann für die Gruppe Schreib- und Lesezugriff festgelegt werden:							
	R	Lesezugriff						
	W	Schreibzugriff						
`edit <Index> [NOAUTH|AUTH|PRIV] [RE|RD|WE|WD]`	Ändert die Sicherheitsstufe der Gruppe und setzt die Zugriffsrechte. Den Index der Gruppe können Sie mit dem Befehl "info" ausgeben.		Die Authentifizierung- und Verschlüsselungseinstellungen können Sie nicht editieren, falls die Gruppe nicht leer ist. Beim Verbieten vom Lesezugriff ist auch der Schreibzugriff verboten. Beim Erlauben vom Schreibzugriff ist auch der Lesezugriff erlaubt.					
			—	✔	✔	✔	✔	✔
	RE	Erlaubt den Lesezugriff						
	RD	Verbietet den Lesezugriff						
	WE	Erlaubt den Schreibzugriff						
	WD	Verbietet den Schreibzugriff						

		Kommentar					
`delete <Index>`	Löscht die SNMPv3 Gruppe an Stelle Index aus der Gruppenliste.	Löschen ist nur dann möglich ist, falls die Gruppe leer ist.					
		—	✔	✔	✔	✔	✔
`clearall`	Löscht alle SNMP-Gruppen, die leer sind.	—	✔	✔	✔	✔	✔

Siehe auch

- Menüpunkt SNMP Config (Seite 113)

5.7.2.9 Menüpunkt CLI\SYSTEM\SNMP\USER

SNMP-Benutzer verwalten

Mit den Befehlen dieses Menüs verwalten Sie SNMP-Benutzer (Anlegen, Löschen usw.).

CLI\SYSTEM\SNMP\USER>

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`add <Benutzername> <Gruppenname> [NONE|MD5|SHA] [Authentifizierungsken.] [Verschlüsselungkennw.]`	Ordnet einen SNMPv3-Benutzer einer Gruppe zu. Falls für die Gruppe Authentifizierung notwendig ist, muss der Algorithmus als Parameter angegeben werden (MD5 oder SHA). Falls für die Gruppe Verschlüsselung notwendig ist, muss das Verschlüsselungskennwort als Parameter angegeben werden.	Das Authentifizierungskennwort und das Verschlüsselungskennwort kann maximal 63 Zeichen lang sein.					
		—	✔	✔	✔	✔	✔
`edit <Index> <Gruppenname> [NONE|MD5|SHA] [Authentifizierungsken.] [Verschlüsselungkennw.]`	Ändert die Gruppenzugehörigkeit, den Authentifizierungsalgorithmus und das Verschlüsselungskennwort des SNMPv3-Benutzers.	—	✔	✔	✔	✔	✔
`delete <Index>`	Löscht einen SNMPv3-Benutzer an der durch den Index angegebenen Stelle aus der Benutzerliste.	—	✔	✔	✔	✔	✔
`clearall`	Löscht alle SNMPv3-Benutzer.	—	✔	✔	✔	✔	✔

Siehe auch

- Menüpunkt SNMP Config (Seite 113)

5.7.2.10 Menüpunkt CLI\SYSTEM\SNMP\TRAP

SNMP-Traps aktivieren, Trapempfänger festlegen

Mit den Befehlen dieses Menüs konfigurieren Sie SNMP-Traps.

CLI\SYSTEM\SNMP\TRAP>

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`traps [E|D]`	Aktiviert / deaktiviert SNMP-Traps.	Traps sind dann aktiviert, falls SNMP v1, v2c auch aktiviert ist.					
		✔	✔	✔	✔	✔	✔
`settrap <entry> <IP-Adresse> <E|D>`	Legt die IP-Adresse des Trap-Empfängers "entry" ("entry" zwischen 1 und 10) fest und aktiviert / deaktiviert die Versendung von Traps an diesen Empfänger.	✔	✔	✔	✔	✔	✔
`clearall`	Löscht alle Einträge aus der trap Konfigurationstabelle.	✔	✔	✔	✔	—	—

Siehe auch

- Menüpunkt SNMP Config (Seite 113)

5.7.2.11 Menüpunkt CLI\SYSTEM\SYSLOG

Zeitsynchronisation im Netzwerk

Mit den Befehlen dieses Menüs legen Sie den SYSLOG-Server und die Logbucheinträge fest.

CLI\SYSTEM\SYSLOG>

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`info`	Zeigt die aktuelle Syslog-Konfiguration an.	✔	✔	✔	✔	✔	✔
`server [IP address]`	Gibt die IP Adresse des Syslog- Servers an.	Nur mit Adminrechten zu ändern.					
		✔	✔	✔	✔	✔	✔
`logs [ D | E ]`	Legt fest ob die Logbucheinträge auch an den Syslog- Server verschickt werden.	Nur mit Adminrechten zu ändern.					
		✔	✔	✔	✔	✔	✔
`auths [ D | E ]`	Legt fest ob die Authentication Logeinträge auch an den Syslog- Server verschickt werden.	Nur mit Adminrechten zu ändern.					
		✔	✔	✔	✔	✔	✔

Siehe auch

- Menüpunkt Syslog (Seite 115)

5.7.2.12 Menüpunkt CLI\SYSTEM\SNTP

Zeitsynchronisation im Netzwerk

Mit den Befehlen dieses Menüs legen Sie den SNTP-Server und die Zeitzone fest.

CLI\SYSTEM\SNTP>

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`server [IP-Adresse]`	IP-Adresse des SNTP-Servers festlegen.	—	✔	✔	✔	✔	✔
`tzone [Stunden]`	Abweichung der Zeitzone des SCALANCE W-700 entsprechend UTC (Universal Time Conversion) in Stunden angeben.	—	✔	✔	✔	✔	✔

Siehe auch

- Menüpunkt SNTP Config (Seite 117)

5.7.2.13 Menüpunkt CLI\SYSTEM\FAULT

Informationen über Fehler

Mit dem Befehl dieses Menüs zeigen Sie Informationen über aufgetretene Fehler an.

CLI\SYSTEM\FAULT>

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`fault [OFF]`	Zeigt den Fehler-Zustand und Fehlerursache. Mit dem Parameter "OFF" setzen Sie die Fehler-LED und den Fehler-Zustand zurück. Vorzugsweise ist aber die Fehlerursache zu beheben.	Man kann die LED und den Fehler-Zustand mit dem Befehl: "fault OFF" zurücksetzen. Vorzugsweise ist aber die Fehlerursache zu beheben.					
		✔	✔	✔	✔	✔	✔
`ipacknow [Index|All]`	Zeigt oder quittiert (löscht) die IP-Alive-Quittungsmeldungen.	Solange nicht alle Fehlermeldungen quittiert sind, bleibt der Fehler-Zustand eingeschaltet. Der Fehlerzustand und die Fault LED erlöschen, falls die einzige Ursache dafür eine IP-Alive Fehlermeldung war. Der Befehl ist im Client-Modus nicht ausführbar.					
		—	—	—	—	✔	✔
`linkack [Index|All]`	Zeigt oder quittiert (löscht) die Link Check-Quittungsmeldungen.	Solange nicht alle Fehlermeldungen quittiert sind, bleibt der Fehler-Zustand eingeschaltet. Der Fehlerzustand und die Fault LED erlöschen, falls die einzige Ursache dafür eine Link Check Fehlermeldung war. Der Befehl ist im Client-Modus nicht ausführbar.					
		—	—	—	—	✔	✔

Siehe auch

- Menüpunkt Fault State (Seite 117)

5.7.2.14 Menüpunkt CLI\SYSTEM\LOADSAVE

Speichern und Laden von Gerätedaten

Mit den Befehlen dieses Menüs speichern Sie Daten aus dem Gerät oder laden Sie Daten in das Gerät (Konfigurationsdaten, Firmware, Authentifizierungsdaten usw.).

CLI\SYSTEM\LOADSAVE>

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`server [IP-Adresse] :[Port-Nummer]`	Legt die IP-Adresse und den Port des TFTP-Servers fest.	✔	✔	✔	✔	✔	✔
`fwname [Dateiname]`	Legt den Namen einer Datei fest, aus der die Firmware geladen wird oder in die die Firmware gespeichert wird. Dieser Namen kann maximal 32 Zeichen lang sein.	✔	✔	✔	✔	✔	✔
`fwload`	Lädt die Firmware aus einer Datei.	✔	✔	✔	✔	✔	✔
`fwsave`	Speichert die Firmware in eine Datei.	✔	✔	✔	✔	✔	✔
`cfgname [Dateiname]`	Legt den Namen einer Datei fest, aus der die Konfigurationsdaten geladen werden oder in die die Konfigurationsdaten gespeichert werden.	✔	✔	✔	✔	✔	✔
`cfgload`	Lädt die Konfigurationsdaten aus einer Datei	✔	✔	✔	✔	✔	✔
`cfgsave`	Speichert die Konfigurationsdaten in eine Datei.	✔	✔	✔	✔	✔	✔
`logname [Dateiname]`	Legt den Namen einer Datei fest, in die die Log-Tabelle gespeichert wird.	✔	✔	✔	✔	✔	✔
`logsave`	Speichert die Log-Tabelle in eine Datei.	✔	✔	✔	✔	✔	✔
`cltcert <Zertifikat>`	Legt den Namen des Zertifikats für den Client fest.	Nur für Clients oder Accesspoints im Client-Modus verfügbar.					
		✔	✔	✔	✔	✔	✔
`cltpass <Passwort>`	Berechtigt zur Benutzung des Zertifikats.	Nur für Clients oder Accesspoints im Client-Modus verfügbar.					
		✔	✔	✔	✔	✔	✔
`cltload`	Lädt das Client-Zertifikat aus einer Datei.	Nur für Clients oder Accesspoints im Client-Modus verfügbar.					
		✔	✔	✔	✔	✔	✔

		Kommentar					
`cltsave`	Speichert das Client-Zertifikat in eine Datei.	Nur für Clients oder Accesspoints im Client-Modus verfügbar.					
		✔	✔	✔	✔	✔	✔
`srvcert <Zertifikat>`	Legt den Namen des Zertifikats für den Server fest.	Nur für Clients oder Accesspoints im Client-Modus verfügbar.					
		✔	✔	✔	✔	✔	✔
`srvload`	Lädt ein Server-Zertifikat aus einer Datei.	Nur für Clients oder Accesspoints im Client-Modus verfügbar.					
		✔	✔	✔	✔	✔	✔
`srvsave`	Speichert das Server-Zertifikat in eine Datei.	Nur für Clients oder Accesspoints im Client-Modus verfügbar.					
		✔	✔	✔	✔	✔	✔
`cltdel`	Löscht Client-Zertifikat.	Nur für Clients oder Accesspoints im Client-Modus verfügbar.					
		✔	✔	✔	✔	✔	✔
`srvdel`	Löscht das Server-Zertifikat.	Nur für Clients oder Accesspoints im Client-Modus verfügbar.					
		✔	✔	✔	✔	✔	✔
`pkgsave`	Speichert das Configuration Package über einem TFTP-Server in eine Datei.	Nur für Clients oder Accesspoints im Client-Modus verfügbar. Ist nur sichtbar, falls ein Zertifikat im Client geladen ist.					
		✔	✔	✔	✔	✔	✔

Hinweis

Die Funktionalität kann über SNMP unter der OID 1.3.6.1.4.1.4196.1.1.4.100.1.5.1.19 (snDownloadEcmCfgPackageControl) bedient werden. Die Bedienung erfolgt analog zu den übrigen OIDs in dieser Gruppe.

Siehe auch

- Menüpunkt Load & Save (Seite 118)

5.7.2.15 Menüpunkt CLI\SYSTEM\CPLUG

Verändern der Daten auf einem C-PLUG

Mit den Befehlen dieses Menüs schreiben Sie Konfigurationsdaten auf einen C-PLUG.

CLI\SYSTEM\CPLUG>

Befehl	Beschreibung		Kommentar					
			IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`initdef`	Initialisiert den C-PLUG neu und kopiert die Default-Konfiguration auf den C-PLUG.		Alle Informationen werden gelöscht.					
			✔	✔	✔	✔	✔	✔
`initmem`	Initialisiert den C-PLUG neu und kopiert die momentan im Gerät gespeicherte Konfiguration auf den C-PLUG.		Alle Informationen werden gelöscht.					
			✔	✔	✔	✔	✔	✔
`bootfrom [MEMORY]`	Zeigt dem Quellmedium, von dem momentan die Konfiguration gelesen wird: C-PLUG oder MEMORY. Der Neustart erfolgt automatisch.		Wenn der C-PLUG gezogen wurde, muss angegeben werden, dass die Konfiguration aus dem internen Speicher gelesen werden soll. Bei gestecktem C-PLUG wird immer versucht, die Konfiguration vom C-PLUG zu lesen. Der Befehl "bootfrom [MEMORY]" ist dann wirkungslos.					
			✔	✔	✔	✔	✔	✔
`cleanplug`	Löscht den C-PLUG.		✔	✔	✔	✔	✔	✔
`preplug <dev>`	Schreibt die Konfigurationsdaten in einen PRESET-PLUG. Der Parameter "dev" gibt dabei an, für welches Gerät der PRESET-PLUG geeignet sein soll:		—	✔	✔	✔	✔	✔
	1	SCALANCE W786-1PRO						
	2	SCALANCE W786-2PRO						
	3	SCALANCE W786-3PRO						
	4	IWLAN/PB-Link						

Siehe auch

- Menüpunkt C-PLUG (Seite 121)

5.7.3 Das Menü CLI\INTERFACES

5.7.3.1 Menüpunkt CLI\INTERFACES\ETHERNET

Einstellungen für WLAN und Ethernet

Mit den Befehlen dieses Menüs konfigurieren Sie die Ethernet-Schnittstelle.

CLI\INTERFACES\ETHERNET>

Befehl	Beschreibung		Kommentar					
			IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`ethspeed [A|100F|100H|10F|10H]`	Legt die Übertragungsgeschwindigkeit und die Betriebsart der Ethernet Schnittstelle fest:		—	✔	✔	✔	✔	✔
			Dieser Befehl ist nur bei den Gerätevarianten mit RJ45-Anschluss verfügbar !					
	A	Automatische Auswahl durch das Gerät						
	100F	100 Mbit/s Vollduplex						
	100H	100 Mbit/s Halbduplex						
	10F	10 Mbit/s Vollduplex						
	10H	10 Mbit/s Halbduplex						
`ethcross [E|D]`	Legt fest, ob an der Ethernet-Schnittstelle ein Crossover-Kabel verwendet wird oder nicht:		—	✔	✔	✔	✔	✔
			Dieser Befehl ist nur möglich, wenn die Übertragungsgeschwindigkeit nicht automatisch vom Gerät festgelegt wird (Befehl "etherspeed" mit dem Parameter "A"). Dieser Befehl ist nur bei den Gerätevarianten mit RJ45-Anschluss verfügbar !					
	D	Standard-Kabel, nicht gekreuzt						
	E	Crossover-Kabel						

Siehe auch

- Menüpunkt Ethernet (Seite 125)

5.7.3.2 Menüpunkt CLI\INTERFACES\WLAN1 (bzw. \WLAN2 oder \WLAN3)

Netzwerkname, Übertragungsverfahren und Kanalwahl

Mit den Befehlen dieses Menüs treffen Sie Festlegungen über die Netzwerkzugehörigkeit und die Kanalwahl.

CLI\INTERFACES\WLAN1> (bzw. \WLAN2 oder \WLAN3)

Befehl	Beschreibung		Kommentar					
			IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`port [E|D]`	Drahtlose Schnittstelle aktivieren / deaktivieren.		—	✔	✔	✔	✔	✔
`ssid [Netzwerkname]`	Vergabe eines Netzwerknamens (SSID).		Nur im Access Point-Modus verfügbar.					
			✔	✔	✔	✔	✔	✔
`mode [A|B|G|H|T|U|X]`	Wählt den Übertragungsstandard aus:		✔	✔	✔	✔	✔	✔
	A	802.11a	Je nach Ländereinstellung sind nicht alle Einstellungen möglich und werden gegebenenfalls abgelehnt. 802.11a/g/h Turbo ist nicht in allen Ländern einstellbar.					
	B	802.11b						
	G	802.11g						
	H	802.11h						
	T	802.11a Turbo						
	U	802.11h Turbo						
	X	802.11g Turbo						
`autoch [E|D]`	Automatische Kanalwahl durch den SCALANCE W78x aktivieren / deaktivieren.		Nur im Access Point-Modus verfügbar.					
			—	—	—	—	✔	✔
`channel [1 ... 167]`	Festlegung des Funk-Kanals.		—	—	—	—	✔	✔
`altchan [Kanal]`	Eingabe der Kanalnummer des alternativen DFS-Kanals.		Nur im Übertragungsstandard 802.11h möglich.					
			—	—	—	—	✔	✔
`adopt [MAC-Adresse]`	MAC-Adresse des Gerätes, welches am Client über Ethernet angeschlossen ist.		Nur im Client-Modus verfügbar.					
			—	✔	✔	✔	✔	✔
`autoadopt [E|D|OWN]`	Automatisches Finden der MAC-Adresse des Gerätes, welches am Client über Ethernet angeschlossen ist. Der Parameter OWN bewirkt, dass sich der Client mit seiner eigenen Ethernet-MAC-Adresse am Access Point anmeldet. Mit dieser Einstellung ist allerdings nur IP-Datenverkehr möglich.		Nur im Client-Modus verfügbar.					
			—	✔	✔	✔	✔	✔
`adhoc [E|D]`	Ad-Hoc- oder Infrastructure-Modus auswählen.		Nur im Client-Modus verfügbar. Nicht bei iPCF.					
			—	✔	✔	✔	✔	✔

		Kommentar					
`anyssid [E|D]`	Mit ANY SSID verbindet sich der Client mit dem besten Access Point in der Umgebung auf den er sich verbinden darf.	Nur im Client-Modus verfügbar. Nicht bei iPCF.					
		✔	✔	✔	✔	✔	✔
`vapno [0 ... 7]`	Festlegung der Anzahl der virtuellen Access Points.	—	—	—	—	✔	✔
`outdoor [E|D]`	Outdoor-AP-Modus aktivieren / deaktivieren.	✔	✔	✔	✔	✔	✔
`802.11G`	Öffnet das Menü "ADVANCED G" (802.11g).	✔	✔	✔	✔	✔	✔
`ADVANCED`	Öffnet das Menü "ADVANCED".	✔	✔	✔	✔	✔	✔
`DATARATES`	Öffnet das Menü "DATARATES".	—	—	—	—	✔	✔
`VAP1`	Öffnet das Menü "VAP1"	Wird nur angezeigt, wenn vapno > 0.					
		—	—	—	—	✔	✔
`VAP2`	Öffnet das Menü "VAP2"	Wird nur angezeigt, wenn vapno > 1.					
		—	—	—	—	✔	✔
`VAP3`	Öffnet das Menü "VAP3"	Wird nur angezeigt, wenn vapno > 2.					
		—	—	—	—	✔	✔
`VAP4`	Öffnet das Menü "VAP4"	Wird nur angezeigt, wenn vapno > 3.					
		—	—	—	—	✔	✔
`VAP5`	Öffnet das Menü "VAP5"	Wird nur angezeigt, wenn vapno > 4.					
		—	—	—	—	✔	✔
`VAP6`	Öffnet das Menü "VAP6"	Wird nur angezeigt, wenn vapno > 5.					
		—	—	—	—	✔	✔
`VAP7`	Öffnet das Menü "VAP7"	Wird nur angezeigt, wenn vapno > 6.					
		—	—	—	—	✔	✔

5.7.3.3 Menüpunkt CLI\INTERFACES\WLAN1\ADVANCED (bzw. \WLAN2\ADVANCED oder \WLAN3\ADVANCED)

Konfiguration des Sendeverhaltens

Mit den Befehlen dieses Menüs legen Sie die Parameter für das Sendeverhalten fest, wie beispielsweise die Paketgröße, ab der fragmentiert wird, oder welche Antenne(n) verwendet werden.

CLI\INTERFACES\WLAN1\ADVANCED> (bzw. \WLAN2\ADVANCED oder \WLAN3\ADVANCED)

Befehl	Beschreibung		Kommentar					
			IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`power [0...4]`	Legt fest, um wieviel dB die Sendeleistung gegenüber der vollen Leistung vermindert wird:		✔	✔	✔	✔	✔	✔
	0	volle Leistung						
	1	-3 dB, half						
	2	-6 dB, quarter						
	3	-9 dB, eights						
	4	minimale Leistung, -12 dB						
`beacon [20 ... 1000]`	Legt das Beacon-Intervall in Millisekunden fest.		—	✔	✔	✔	✔	✔
`dtim [1 ... 255]`	Legt die Data Beacon Rate fest.		Nur im Access Point-Modus verfügbar.					
			—	—	—	—	✔	✔
`rtsthr [1 ... 2346]`	Legt die Paketgröße fest, ab der das RTS/CTS-Verfahren angewendet wird.		—	✔	✔	✔	✔	✔
`fragthr [256 ... 2346]`	Legt die Größe fest, ab der Pakete fragmentiert werden.		Nicht bei iPCF					
			—	✔	✔	✔	✔	✔
`bkscan [D|I|A]`	Legt den Modus fest, wie der Client nach weiteren Access Points sucht.		—	✔	✔	✔	✔	✔
	D	Disabled	Nur im Client-Modus verfügbar. Nicht bei iPCF					
	I	Scan if idle						
	A	Scan always						
`bkscanint [200 ... 60000]`	Intervall, in dem der Client nach weiteren Access Points sucht.		Nur im Client-Modus verfügbar. Nicht bei iPCF					
			—	✔	✔	✔	✔	✔
`bkchannel [Kanäle]`	Auswahl bestimmter Kanäle, auf denen der Client nach weiteren Access Points sucht. Die Kanäle sind durch Leerzeichen getrennt einzutragen		Nur im Client-Modus verfügbar.					
			✔	✔	✔	✔	✔	✔

			Kommentar					
`bkchsel [E|D]`	Aktiviert / deaktiviert das Suchen nach weiteren Access Points auf bestimmten Kanälen.		Nur im Client-Modus verfügbar.					
			✔	✔	✔	✔	✔	✔
`force [E|D]`	Aktiviert / deaktiviert Roaming bei Verbindungsabbruch auf der Ethernet-Schnittstelle.		Nur im Access Point-Modus verfügbar.					
			—	—	—	—	✔	✔
`roamthr`	Bestimmt die Schwelle, ab der ein Client zu einem anderen AP wechselt.		✔	✔	✔	✔	✔	✔
	low	Wechselt schon bei geringfügig höherer Feldstärke zum AP mit stärkerem Signal.						
	medium	Wechselt bei mäßig höherer Feldstärke zum AP mit stärkerem Signal.						
	high	Wechselt erst bei deutlich höherer Feldstärke zum AP mit stärkerem Signal.						
`swretry [E|D]`	Aktiviert / deaktiviert die Funktionalität SW-Wiederholung.		Nicht bei iPCF					
			—	✔	✔	✔	✔	✔
`swretno [0 ... 15]`	Bestimmt die Anzahl der SW-Wiederholungen.		✔	✔	✔	✔	✔	✔
`hwretno [0 ... 15]`	Bestimmt die Anzahl der HW-Wiederholungen.		Nicht bei iPCF					
			—	✔	✔	✔	✔	✔
`preamb [E|D]`	Aktiviert / deaktiviert die kurze Preambel.		Bei Aktivierung dieser Funktion werden höhere Datenraten nach IEEE 802.11b unterstützt (höhere Performance).					
			✔	✔	✔	✔	✔	✔
`antenna [A|B|SA|SB|D]`	Legt fest, welche Antennen verwendet werden:		✔	✔	✔	✔	✔	✔
	A	Nur Antenne A	Beim IWLAN/PB-Link mit einer Antennenbuchse darf die Voreinstellung (Antenne A) nicht verändert werden.					
	B	Nur Antenne B						
	SA	Antenne A senden, Antenne B empfangen.						
	SB	Antenne B senden, Antenne A empfangen.						
	D	Die beste der beiden Antennen verwenden (Antennen-Diversity).						
`noise [A|L|M|H]11`	Einstellen des Noise Filters.		✔	✔	✔	✔	✔	✔
	A	Automatisch	Eine starke Noise Filterung ermöglicht eine stabilere Verbindung, jedoch auch eine geringere Reichweite.					
	L	Low						
	M	Medium						

			Kommentar					
	H	High						
`wmm [E|D]`	Aktiviert / deaktiviert die Telegrammübertragung unter Berücksichtigung der Priorität.		Nicht bei iPCF					
			✔	✔	✔	✔	✔	✔
`antgain [0...30]`	Eingabe des Antennen-Gewinns dBi.		✔	✔	✔	✔	✔	✔
`anttype [0...n]`	Eingabe des Antennen-Typs:		✔	✔	✔	✔	✔	✔
	0	User defined	Zum Anzeigen der Liste geben Sie "anttype ?" ein.					
	1	ANT792-6MN - gain: 6 dBi (2,4 GHz)						
	2	ANT793-6MN - gain: 6 dBi (5 GHz)						
	3	ANT795-6MN - gain: 6 dBi (2,4 GHz) 8 dBi (5 GHz)						
	4	ANT795-6DN - gain: 9 dBi (2,4 GHz) 9 dBi (5 GHz)						
	5	ANT792-8DN - gain: 14 dBi (2,4 GHz)						
	6	ANT793-8DN - gain: 18 dBi (5 GHz)						
	7	ANT792-4DN (RCoax Antenna) - gain: 4 dBi (2,4 GHz)						
	8	ANT793-4MN (RCoax Antenna) - gain: 6 dBi (5 GHz)						
	9	RCoax leaky wave cable - gain: 0 dBi (2,4 GHz) 0dBi (5 GHz)						
	10	ANT795-4MR gain: 3 dBi (2,4 GHz) 5 dBi (5 GHz)						
	11	ANT795-4MS gain: 4 dBi (2,4 GHz) 5 dBi (5 GHz)						
`antcable [0 ... 30]`	Eingabe der Länge des Antennenkabels in Meter.		✔	✔	✔	✔	✔	✔

5.7.3.4 Menüpunkt CLI\INTERFACES\WLAN1\SSID (bzw. \WLAN2\SSID oder \WLAN3\SSID)

Verbindung zu einem Netzwerk

Mit den Befehlen dieses Menüs konfigurieren Sie, wie sich ein Client mit einem Netzwerk verbindet.

Hinweis

Der Untermenüpunkt SSID List ist nur für Clients oder Access Points im Client-Modus verfügbar.

CLI\INTERFACES\WLA1\SSID> (bzw. \WLAN2\SSID oder \WLAN3\SSID)

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`add <Netzwerkname>`	Fügt einen Netzwerknamen (SSID) in die SSID Liste ein.	Nur im Client-Modus verfügbar.					
		✔	✔	✔	✔	✔	✔
`edit <index> <Netzwerkname>`	Ändert den Netzwerknamen (SSID) an Stelle <index> in die SSID Liste.	Nur im Client-Modus verfügbar.					
		✔	✔	✔	✔	✔	✔
`delete <index>`	Löscht den Netzwerknamen (SSID) an Stelle <index> aus der SSID Liste.	Nur im Client-Modus verfügbar.					
		✔	✔	✔	✔	✔	✔
clearall	Löscht alle Netzwerknamen (SSID) aus der SSID Liste.	✔	✔	✔	✔	—	—

Siehe auch

- Menüpunkt SSID List (Seite 133)

5.7.3.5 Menüpunkt CLI\INTERFACES\WLAN1\802.11G (bzw. \WLAN2\802.11G oder \WLAN3\802.11G)

Spezielle Möglichkeiten des 802.11g-Standards

Mit den Befehlen dieses Menüs können Sie die spezifischen Eigenschaften des Standards 802.11g konfigurieren. Beispielsweise können Sie festlegen, wie Management- und Kontrolldaten im 802.11g-Modus versendet werden.

CLI\INTERFACES\WLAN1\802.11G (bzw. \WLAN2\802.11G oder \WLAN3\802.11G)

Befehl	Beschreibung		Kommentar					
			IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`ctsmode [0|1|2]`	Legt fest, ob das RTS/CTS-Verfahren bei 802.11g Paketen angewendet wird:		—	—	—	—	✔	✔
	0	Kein CTS verwenden.	Nur im Access Point-Modus verfügbar.					
	1	Immer CTS verwenden.						
	2	CTS abhängig ob 802.11b Clients vorhanden sind.						
`ctsrate [0|1|2|3]`	Bestimmt die Datenrate für 802.11g-CTS-Telegramme:		✔	✔	✔	✔	✔	✔
			Nicht bei iPCF					
	0	1 Mbit/s						
	1	2 Mbit/s						
	2	5,5 Mbit/s						
	3	11 Mbit/s						
`ctstype [0|1]`	Bestimmt das Verfahren zur Kollisionsvermeidung für 802.11g-Paketen:		✔	✔	✔	✔	✔	✔
			Nicht bei iPCF					
	0	Nur CTS						
	1	RTS/CTS						
`sslot [E|D]`	Aktiviert / deaktiviert verkürzte Pausenzeiten zwischen Datenpaketen ("Short Slot Time").		✔	✔	✔	✔	✔	✔
`only11g [E|D]`	Wenn aktiviert, wird nur das OFDM-Modulationsverfahren unterstützt.		Nur im Access Point-Modus verfügbar.					
			—	—	—	—	✔	✔

5.7.3.6 Menüpunkt CLI\INTERFACES\WLAN1\DATARATES (bzw. \WLAN2\DATARATES oder \WLAN3\DATARATES)

Variable Einstellung der Übertragungsraten

Mit den Befehlen dieses Menüs können Sie die Übertragungsrate festlegen.

CLI\INTERFACES\WLAN1\DATARATES (bzw. \WLAN2\DATARATES oder \WLAN3\DATARATES)

<table>
<tr><th rowspan="2">Befehl</th><th colspan="3" rowspan="2">Beschreibung</th><th colspan="6">Kommentar</th></tr>
<tr><th>IWLAN/ PB LINK</th><th>W744</th><th>W746</th><th>W747</th><th>W78x</th><th>W78x RR</th></tr>
<tr><td>info</td><td colspan="3">Die nachfolgende Übersicht zeigt die verfügbaren Übertragungsraten und deren aktuelle Konfiguration an.</td><td>—</td><td>—</td><td>—</td><td>—</td><td>✔</td><td>✔</td></tr>
<tr><td>default</td><td colspan="3">Aktiviert die Standardeinstellung für den aktuellen WLAN-Modus</td><td>—</td><td>—</td><td>—</td><td>—</td><td>✔</td><td>✔</td></tr>
<tr><td rowspan="14">edit <Rate> <E | D> <E | D></td><td colspan="3">Ändert die Einstellungen für die angegebene Datenrate (in Mbit/s). Die beiden Parameter geben an, ob die Rate verwendet werden soll bzw. als "Basic Rate" definiert ist.
Übersicht:</td><td>—</td><td>—</td><td>—</td><td>—</td><td>✔</td><td>✔</td></tr>
<tr><td>Rate</td><td>Enabled</td><td>Basic Rate</td><td colspan="6" rowspan="13">Bsp.:
Über den Befehl
"edit 5.5 d d"
wird die Datenrate 5.5 Mbit/s deaktiviert. Der Screenshot zeigt die Standardeinstellung für den Modus 802.11g.</td></tr>
<tr><td>1</td><td>X</td><td>X</td></tr>
<tr><td>2</td><td>X</td><td>X</td></tr>
<tr><td>5.5</td><td>X</td><td>X</td></tr>
<tr><td>6</td><td>X</td><td></td></tr>
<tr><td>9</td><td>X</td><td></td></tr>
<tr><td>11</td><td>X</td><td>X</td></tr>
<tr><td>12</td><td>X</td><td></td></tr>
<tr><td>18</td><td>X</td><td></td></tr>
<tr><td>24</td><td>X</td><td></td></tr>
<tr><td>36</td><td>X</td><td></td></tr>
<tr><td>48</td><td>X</td><td></td></tr>
<tr><td>54</td><td>X</td><td></td></tr>
</table>

Siehe auch

- Menüpunkt Data Rates (Seite 135)

5.7.3.7 Menüpunkt CLI\INTERFACES\WLAN1\VAP1..7 (bzw. \WLAN2\VAP1..7 oder \WLAN3\VAP1..7)

Virtuelle Access Points

Mit den Befehlen dieses Menüs treffen Sie Festlegungen für virtuelle Access Points.

CLI\INTERFACES\WLAN1\VAP1..7> (bzw. \WLAN2\VAP1..7 oder \WLAN3\VAP1..7)

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`vap [E|D]`	Virtuellen Access Point aktivieren / deaktivieren.	Nur im Access Point-Modus verfügbar.					
		—	—	—	—	✔	✔
`ssid [Netzwerkname]`	Vergabe eines Netzwerknamens (SSID).	Nur im Access Point-Modus verfügbar.					
		—	—	—	—	✔	✔

Siehe auch

- Menüpunkt VAP (Seite 136)

5.7.4 Das Menü CLI\SECURITY

5.7.4.1 Menüpunkt CLI\SECURITY

Konfiguration des SCALANCE W-700

Mit dem Befehl dieses Menüs legen Sie fest, wie die Konfiguration des SCALANCE W-700 erfolgen soll.

CLI\SECURITY>

Befehl	Beschreibung		Kommentar					
			IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`mgmteth [E|D]`	Die Konfiguration des SCALANCE W-700 ist:		—	✔	✔	✔	✔	✔
	E	nur über die drahtgebundene Ethernet-Schnittstelle möglich.						
	D	über alle Schnittstellen möglich						

Siehe auch

- Menüpunkt Security (Seite 137)

5.7.4.2 Menüpunkt CLI\SECURITY\BASIC\WLAN1 (bzw. \WLAN2 oder \WLAN3)

Security-Einstellungen des SCALANCE W-700

Mit den Befehlen dieses Menüs legen Sie die Security-Einstellungen des SCALANCE W-700 fest.

CLI\SECURITY\BASIC\WLAN1> (bzw. \WLAN2 oder \WLAN3)

Befehl	Beschreibung		Kommentar					
			IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`authent [0|1|2|3|4|5|6|7|8]`	Authentifizierungstyp festlegen. Geben Sie als Parameter n eine Zahl zwischen 0 und 4 für die Art der Authentifizierung an:		✔	✔	✔	✔	✔	✔
	0	Open System	Bei den Authentifizierungstypen 7 (WPA-Auto) und 8 (WPA-Auto-PSK) muss das jeweilige Verschlüsselungsverfahren von WPA und WPA2 bzw. von WPA-PSK & WPA2-PSK gleich sein. Nicht bei iPCF					
	1	Shared Key						
	2	WPA (RADIUS)						
	3	WPA-PSK						
	4	802.1x (RADIUS)						
	5	WPA2						
	6	WPA2-PSK						
	7	WPA-Auto						
	8	WPA-Auto-PSK						
`encrypt [E|D]`	Verschlüsselung aktiviert/deaktivieren.		✔	✔	✔	✔	✔	✔
`cipher [OFF|AUTO|WEP|AES|TKIP]`	Verschlüsselungsverfahren festlegen.		✔	✔	✔	✔	✔	✔
`keysrc [0..2]`	Schlüsselquelle auswählen. Geben Sie als Parameter 0 ein, wenn der Schlüssel vom Server verwaltet wird. Geben Sie 1 ein, wenn der Schlüssel von einem RADIUS Server kommen soll. Geben Sie 2 ein, wenn ein Mischbetrieb gewählt wird.		✔	✔	✔	✔	✔	✔
`defkey [1|2|3|4]`	Auswahl des Default-WEPSchlüssels.		✔	✔	✔	✔	✔	✔
`wpaphrase [WPA-Passwort]`	Eingabe des WPA-PSK-Passworts.		Das Passwort kann 8 bis 63 ASCII-Zeichen oder genau 64 hexadezimale Zeichen lang sein.					
			✔	✔	✔	✔	✔	✔
`grkint [Intervall]`	Festlegung des "Group Key Update Intervals" bei WPA-PSK.		Intervall in Sekunden, (0; 36…36000), 0 = AUS					
			—	—	—	—	✔	✔
`supssid [E|D]`	Funktionalität Close Wireless System aktivieren / deaktivieren.		—	—	—	—	✔	✔
`intracom [A|I|E]`	Allowed / Intracell or Ethernet blocking)		—	—	—	—	✔	✔

			Kommentar					
	Allowed	keine Einschränkung des Datenverkehrs						
	Intracell	Blockieren des Datenverkehrs zwischen den Clients in der Funkzelle						
	Ethernet	Blockieren des Datenverkehrs zum Ethernet						
`ssidcom [E|D]`	(Enable / Disable communication to other SSIDs)		—	—	—	—	✔	✔
	Enable	Datenverkehr zu anderen SSIDs erlaubt						
	Disable	Datenverkehr zu anderen SSIDs blockiert						
`username [Name]`	Festlegung des Benutzernamens für RADIUS-Server.		Nur im Client-Mode.					
			✔	✔	✔	✔	✔	✔
`password [Passwort]`	Festlegung des Passworts für RADIUS-Server.		Nur im Client-Mode.					
			✔	✔	✔	✔	✔	✔
`chkserver [E|D]`	Aktiviert / deaktiviert die Authentifizierung des Servers.		Nur im Client-Mode.					
			✔	✔	✔	✔	✔	✔
`radauth`	Setzt den RADIUS Authentifizierungstyp auf AUTO EAP_TLS EAP_TTLS PEAP		✔	✔	✔	✔	✔	✔
`preauth`	Aktiviert die Preauthentication für WPA2		✔	✔	✔	✔	—	—
`aging`	Setzt bei WPA2 den Erneuerungsintervall für den PMK in Minuten		✔	✔	✔	✔	—	—

5.7.4.3 Menüpunkt CLI\SECURITY\BASIC\WLAN1\VAP1..7 (bzw. \WLAN2\VAP1..7 oder \WLAN3\VAP1..7)

Security-Einstellungen des virtuellen Access Point

Mit den Befehlen dieses Menüs legen Sie die Security-Einstellungen des virtuellen Access Point fest.

CLI\SECURITY\BASIC\WLAN1\VAP1> (bzw. \WLAN2\VAP1 oder \WLAN3\VAP1)

Befehl	Beschreibung		Kommentar					
			IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`authent [0|1|2|3|4|5|6|7|8]`	Authentifizierungstyp festlegen. Geben Sie als Parameter n eine Zahl zwischen 0 und 4 für die Art der Authentifizierung an:		—	—	—	—	✔	✔
	0	Open System	Bei den Authentifizierungstypen 7 (WPA-Auto) und 8 (WPA-Auto-PSK) muss das jeweilige Verschlüsselungsverfahren von WPA und WPA2 bzw. von WPA-PSK & WPA2-PSK gleich sein.					
	1	Shared Key						
	2	WPA (RADIUS)						
	3	WPA-PSK						
	4	802.1x (RADIUS)						
	5	WPA2						
	6	WPA2-PSK						
	7	WPA-Auto						
	8	WPA-Auto-PSK						
`encrypt [E|D]`	Verschlüsselung aktiviert/deaktivieren.		—	—	—	—	✔	✔
`cipher [OFF|AUTO|WEP|AES|TKIP]`	Verschlüsselungsverfahren festlegen.		—	—	—	—	✔	✔
`defkey [1|2|3|4]`	Auswahl des Default-WEPSchlüssels.		—	—	—	—	✔	✔
`wpaphrase [WPA-Passwort]`	Eingabe des WPA-PSK-Passworts.		Das Passwort kann 8 bis 63 ASCII-Zeichen oder genau 64 hexadezimale Zeichen lang sein.					
			—	—	—	—	✔	✔
`grkint [Intervall]`	Festlegung des "Group Key Update Intervals" bei WPA-PSK.		Intervall in Sekunden, (0; 36…36000), 0 = AUS					
			—	—	—	—	✔	✔
`supssid [E|D]`	Funktionalität Close Wireless System aktivieren / deaktivieren.		—	—	—	—	✔	✔

5.7.4.4 Menüpunkt CLI\SECURITY\KEYS\WLAN1 (bzw. \WLAN2 oder \WLAN3)

Festlegung des WEP-Schlüssels

Mit den Befehlen dieses Menüs tragen Sie einen Schlüssel in die Schlüsseltabelle ein und bearbeiten diesen.

CLI\SECURITY\KEYS\WLAN1> (bzw. \WLAN2 oder \WLAN3)

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`add <Len> <Key> [Index]`	Fügt einen Schlüssel ans Ende oder am angegebenen Index der Tabelle ein.	Index ab 5 sind Private Keys					
		—	—	—	—	✔	✔
`edit <Index> <Len> <Key>`	Verändert den Schlüssel an der Stelle Index.	✔	✔	✔	✔	✔	✔
`delete <Index>`	Löscht den Schlüssel an der Stelle Index.	✔	✔	✔	✔	✔	✔
`clearall`	Löscht alle Schlüssel.	✔	✔	✔	✔	✔	✔

Siehe auch

- Menüpunkt Keys (Seite 142)

5.7.4.5 Menüpunkt CLI\SECURITY\ACL\WLAN1 (bzw. \WLAN2 oder \WLAN3)

Bearbeitung der Acess Control List (ACL)

Mit den Befehlen dieses Menüs bearbeiten Sie Einträge in der Access Control List.

CLI\SECURITY\ACL\WLAN1> (bzw. \WLAN2 oder \WLAN3)

Befehl	Beschreibung		Kommentar					
			IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`aclmode [E|D|S]`	Globale Freigabe der ACL:		—	—	—	—	✔	✔
	E	Enable	Nur im Access Point-Modus					
	D	Disable						
	S	Strict						
`add <MAC> [A|Y|K|P][Key]`	Erstellen eines neuen Eintrags in der ACL:		—	—	—	—	✔	✔
	MAC	MAC-Adresse des Client	Nur im Access Point-Modus					
	A	Allow						
	Y	Deny						
	K	Default Key						
	P	Private Key						
	Key	Key index für Private Key						
`edit <index> [E|D] [A|Y|K|P] [Key]`	Ändern eines vorhandenen ACL Eintrags:		—	—	—	—	✔	✔
	index	Nummer des ACL-Eintrags	Nur im Access Point-Modus					
	E	Enable						
	D	Disable						
	A	Allow						
	Y	Deny						
	K	Default Key						
	P	Private Key						
	Key	Key index für Private Key						
`delete <index>`	Löschen eines vorhandenen ACL Eintrags: index Nummer des ACL Eintrags		Nur im Access Point-Modu					
			—	—	—	—	✔	✔
`clearall`	Löscht alle ACL Einträge.		Nur im Access Point-Modus					
			—	—	—	—	✔	✔

Siehe auch

- Menüpunkt ACL (Seite 143)

5.7.4.6 Menüpunkt CLI\SECURITY\RADIUS

Authentifizierung über einen externen Server

Mit den Befehlen dieses Menüs legen Sie z. B. IP-Adressen, Ports und Passwort fest.

CLI\SECURITY\RADIUS>

Befehl	Beschreibung		Kommentar					
			IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`server [IP-Adresse]`	Legt die IP-Adresse des primären RADIUS-Server fest.		—	—	—	—	✔	✔
`server B [IP-Adresse]`	Legt IP-Adresse des Backup-RADIUS-Server fest.		—	—	—	—	✔	✔
`port [Port]`	Legt den Port des primären RADIUS-Server fest.		—	—	—	—	✔	✔
`port B [Port]`	Legt den Port des Backup-RADIUS-Server fest.		—	—	—	—	✔	✔
`secret [Passwort]`	Legt das Passwort für den primären RADIUS-Server fest.		—	—	—	—	✔	✔
`secret B [Passwort]`	Legt das Passwort für den Backup-RADIUS-Server fest.		—	—	—	—	✔	✔
`maxreq [max. Anzahl]`	Maximale Anzahl der Anfragen an den RADIUS-Server.		—	—	—	—	✔	✔
`maxreq B [max. Anzahl]`	Maximale Anzahl der Anfragen an den RADIUS-Server (Backup-Server).		—	—	—	—	✔	✔
`authprd [Zeit in s]`	Zeitdauer für die Wiederholung der Authentifizierung.		Der Defaultwert beträgt 3600 s					
			—	—	—	—	✔	✔
`Time_scr [S|L]`	Legt die Zeit für die Reauthorisierung fest.		—	—	—	—	✔	✔
	S	Server						
	L	Lokal						

Siehe auch

- Menüpunkt RADIUS Server (Seite 145)

5.7.4.7 Menüpunkt CLI\SECURITY\ACCESS

Zugriffsrechte für IP-Adressen

Mit den Befehlen dieses Menüs bestimmen Sie Zugriffsrechte für IP-Adressen.

CLI\SECURITY\ACCESS>

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`access [E|D]`	Access Control Liste aktivieren/deaktivieren.	—	✔	✔	✔	✔	✔
`statmgmt [A|D]`	Auf die IP-Adressen der Access Control Liste kann zugegriffen / nicht zugegriffen werden (Accessed / Denied).	—	✔	✔	✔	✔	✔
`add <IP>`	Fügt eine neue IP-Adresse hinzu.	—	✔	✔	✔	✔	✔
`edit <Index|IP> [E|D]`	Aktiviert / deaktiviert den über den Index oder der IP-Adresse angegebenen Eintrag in der Tabelle.	—	✔	✔	✔	✔	✔
`delete <Index|IP>`	Löscht den Eintrag.	—	✔	✔	✔	✔	✔
`edit_r [E|D] [IP_1 IP_2]`	Fügt einen neuen IP-Bereich hinzu bzw. bearbeitet diesen.	—	✔	✔	✔	✔	✔
`clearall`	Access Control Liste löschen.	—	✔	✔	✔	✔	✔
`delete_r`	Löscht einen IP-Bereich.	—	✔	✔	✔	✔	✔
`clear_r`	Löscht alle IP-Bereiche.	—	✔	✔	✔	✔	✔

Siehe auch

- Menüpunkt Access (Seite 146)

5.7.5 Das Menü CLI\BRIDGE

5.7.5.1 Menüpunkt CLI\BRIDGE

Löschen veralteter Bridge-Informationen

Mit dem Befehl dieses Menüs legen Sie fest, nach welcher Zeit veraltete Bridge-Informationen in der Learning Table gelöscht werden.

CLI\BRIDGE>

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`aging [E|D|Aging time]`	Aktiviert / deaktiviert das automatische Löschen von Informationen über die Zuordnung von MAC-Adressen und Ports. Mit dem Parameter Aging time können Sie die Zeit verändern.	Für die Aging time sind Werte zwischen 10 s und 1.000.000 s möglich. Der Defaultwert ist 300 s (5 min).					
		—	✔	✔	✔	✔	✔
`learn`	Zeigt die Learning table an.	—	✔	✔	✔	—	—
`arp`	Zeigt die ARP table an.	—	✔	✔	✔	✔	✔
`ipmap`	Zeigt die IP Mapping table an	—	✔	✔	✔	—	—
`STORMTHR`	Öffnen des Storm Threshold Menüs	—	✔	✔	✔	—	—
`NAT`	Öffnen des NAT Menüs	—	✔	✔	✔	—	—

Siehe auch

- Menüpunkt Bridge (Seite 147)

5.7.5.2 Menüpunkt CLI\BRIDGE\WDS\WLAN1 (bzw. \WLAN2 oder \WLAN3)

Reichweitenvergrößerung mit WDS

Mit den Befehlen dieses Menüs legen Sie die Betriebsart WDS (Wireless Distributed System) zum Zweck der Reichweitenvergrößerung oder zum Aufbau eines Wireless-Backbones fest.

CLI\BRIDGE\WDS\WLAN1>-(bzw. \WLAN2 oder \WLAN3)

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`edit <Index> [E|D] [SE|SD] [Key]`	Verändert die mit Index angegebene WDS-Verbindung. Mit [E|D] können Sie die Verbindung aktivieren / deaktivieren.	—	—	—	—	✔	✔
`delete <Index>`	Löscht die Verbindung mit dem angegebenen Index.	—	—	—	—	✔	✔
`clearall`	Löscht alle WDS-Verbindungen.	—	—	—	—	✔	✔

Siehe auch

- Menüpunkt WDS (Seite 148)

5.7.5.3 Menüpunkt CLI\BRIDGE\VLAN\VLAN_ID

VLAN

Mit den Befehlen dieses Menüs legen Sie die VLAN-IDs fest.

CLI\BRIDGE\VLAN\VLAN_ID>

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`info`	Zeigt die aktuell projektierten VLANs in Bezug zu den Ports an.	—	—	—	—	✔	✔
`add <VLAN-ID> [u [Ports]]`	Fügt ein neues VLAN hinzu. Ports: Angabe der Ports, die für das VLAN projektiert werden. u: Der Port ist Mitglied des VLANs, Telegramme werden ohne VLAN-Tag gesendet. Beispiele: add 100 u 2 4 Legt einen Eintrag mit der VLAN-ID 100 an. Die Ports 2 und 4 sind Mitglieder dieses VLANs.	—	—	—	—	✔	✔
`edit <VLAN-ID> [- [Ports],] [u [Ports],]`	Ändert die Zugehörigkeit von Ports zu einem VLAN. Die Parameter entsprechen denen des Befehls add. Beispiele: edit 100 - 2 Der Port 2 gehört nicht mehr zum VLAN mit der ID 100.	—	—	—	—	✔	✔
`delete <VLAN-ID>`	Löscht das VLAN mir der angegebenen VLAN-ID aus der Konfiguration des SCALANCE W78x.	—	—	—	—	✔	✔

Siehe auch

- Menüpunkt VLAN (Seite 151)

5.7.5.4 Menüpunkt CLI\BRIDGE\VLAN\PORTS

VLAN Ports

Mit den Befehlen dieses Menüs legen Sie die Eigenschaften des VLAN-Ports fest.

CLI\BRIDGE\VLAN\PORTS>

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`Info`	Zeigt eine Übersicht der Ports und der zugehörigen VLAN-Einstellungen.	—	—	—	—	✔	✔
`vlan <Port> <E|D>`	Aktiviert bzw. deaktiviert VLAN für den angegebenen Port.	—	—	—	—	✔	✔
`portvid <Port> <VLAN-ID>`	Empfangene Telegramme ohne VLAN-Tag bekommen an dem angegebenen Port ein VLAN-Tag mit der <VLAN ID>.	—	—	—	—	✔	✔
`portprio <Port> <Priority>`	Die Priorität gemäß 802.1d, mit der ungetaggte Frames versehen werden.	—	—	—	—	✔	✔
`member <Port> <all|specific>`	Der angegebene Port ist Mitglied von allen VLANs (all) oder nur den unter VLAN-ID konfigurierten (specific, siehe oben).	—	—	—	—	✔	✔

Siehe auch

- Menüpunkt VLAN (Seite 151)

5.7.5.5 Menüpunkt CLI\BRIDGE\SPANNING

Spanning Tree Eigenschaften

Mit den Befehlen dieses Menüs legen Sie die Spanning Tree Eigenschaften fest.

CLI\BRIDGE\SPANNING>

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`info`	Zeigt die aktuelle Spanning Tree-Konfiguration an.	—	—	—	—	✔	✔
`spanning [E | D]`	Schaltet den (R)STP Algorithmus an (E) oder aus (D).	—	—	—	—	✔	✔
`version [R | S]`	Legt fest ob Rapid Spanning Tree (R) oder Spanning Tree (S) Modus gefahren wird.	—	—	—	—	✔	✔
`bridge [0...61440]`	Legt die Bridgepriorität für den SCALANCE W-700 fest.	Default-Wert: 32768					
		—	—	—	—	✔	✔
`hellotm [1...10]`	Legt den Zeitabstand zwischen zwei BPDU-Telegrammen in Sekunden fest.	Default-Wert: 2 s					
		—	—	—	—	✔	✔
`fwd_delay [4...30]`	Legt die Verzögerungszeit für die Wirksamkeit von Konfigurationsinformationen fest (Angabe in Sekunden).	Default-Wert: 15 s					
		—	—	—	—	✔	✔
`maxage [6....40]`	Maximales Alter für Konfigurations-Informationen. (Angabe in Sekunden).	Default-Wert: 20 s					
		—	—	—	—	✔	✔

Siehe auch

- Menüpunkt Spanning Tree (Seite 158)

5.7.5.6 Menüpunkt CLI\BRIDGE\SPANNING\PORTS

Spanning Tree Ports

Mit den Befehlen dieses Menüs legen Sie die Spanning Tree Port-Eigenschaften fest.

CLI\BRIDGE\SPANNING\PORTS>

Befehl	Beschreibung		Kommentar					
			IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`info`	Zeigt die aktuelle Spanning Tree-Konfiguration für alle Ports an.		—	—	—	—	✔	✔
`portstp <E|D> [Ports]`	Aktiviert / deaktiviert der Spanning Tree-Algorithmus für die angegebenen Ports.		—	—	—	—	✔	✔
`portprio <Port> [0 ... 240]`	Legt die Priorität für den Port fest.							
			—	—	—	—	✔	✔
`stp_cost <Port> [1 ... 65535]`	Legt die Pfadkosten für den Port fest, falls die Version auf STP eingestellt ist.							
			—	—	—	—	✔	✔
`rstp_cost <Port> [0 ... 200000000]`	Legt die Pfadkosten für den Port fest, falls die Version auf RSTP eingestellt ist. Bei einem Wert von 0 wird der Wert berechnet.							
			—	—	—	—	✔	✔
`edgeport <Port> [T|F]`	Gibt an, ob an diesem Port ein Endgerät (T) oder eine Station (F) angeschlossen ist, die Spanning Tree bzw. Rapid Spanning Tree unterstützt. Wird ein (Rapid) Spanning Tree-Protokoll empfangen, wird automatisch der Wert F angezeigt.		—	—	—	—	✔	✔
`ptpport <Port> <A|T|F>`	Die Point-to-Point-Verbindung stellt eine direkte Verbindung zwischen zwei Stationen dar. Für diesen Fall gibt es folgende Einstellmöglichkeiten:		—	—	—	—	✔	✔
	A	Der Port erkennt anhand der Duplexität einen PtP-Port. Bei Vollduplex wird eine PtP-Verbindung angenommen, bei Halbduplex kein PtP-Verbindung (shared medium).						
	T	Legt auch bei Halbduplex eine PtP-Verbindung fest.						
	F	Legt fest, dass über den betreffenden Port auch bei Vollduplex keine PtP-Verbindung besteht.						

Siehe auch

- Menüpunkt Spanning Tree (Seite 158)

5.7.5.7 Menüpunkt CLI\BRIDGE\STORMTHR

Storm Threshold

Mit den Befehlen dieses Menüs legen Sie die Storm Threshold Eigenschaften fest.

CLI\BRIDGE\STORMTHR>

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`stormthr <E|D>`	Aktiviert / deaktiviert die Storm Threshold-Funktion.	✔	✔	✔	✔	✔	✔
`broadcast <Grenzwert>`	Legt die maximale Anzahl von Broadcast-Pakete pro Sekunde von der gleichen Adresse fest.	✔	✔	✔	✔	✔	✔
`multicast <Grenzwert>`	Legt die maximale Anzahl von Multicast-Pakete pro Sekunde von der gleichen Adresse fest.	✔	✔	✔	✔	✔	✔
`broad_eth <Grenzwert>`	Legt die maximale Anzahl von Broadcast-Pakete pro Sekunde für die Ethernet-Schnittstelle festlegen.	✔	✔	✔	✔	✔	✔
`multi_eth <Grenzwert>`	Legt die maximale Anzahl von Multicast-Pakete pro Sekunde für die Ethernet-Schnittstelle festlegen.	✔	✔	✔	✔	✔	✔
`broad_1 <Grenzwert>` `broad_2 <Grenzwert>`	Legt die maximale Anzahl von Broadcast-Pakete pro Sekunde für die erste bzw. zweite Funk-Schnittstelle festlegen.	✔	✔	✔	✔	✔	✔
`multi_1 <Grenzwert>` `multi_2 <Grenzwert>`	Legt die maximale Anzahl von Multicast-Pakete pro Sekunde für die erste bzw. zweite Funk-Schnittstelle festlegen.	✔	✔	✔	✔	✔	✔

Siehe auch

- Menüpunkt Storm Threshold (Seite 166)

5.7.5.8 Menüpunkt CLI\BRIDGE\NAT

NAT (Network Adress Translation)

Mit den Befehlen dieses Menüs legen Sie die NAT Eigenschaften fest.

CLI\BRIDGE>nat

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`nat [E|D]`	Aktiviert / deaktiviert NAT	✔	✔	✔	✔	✔	✔
`ip [IP address]`	Setzt die lokale IP-Adresse für den Ethernet-Port	✔	✔	✔	✔	✔	✔
`subnet [Subnet mask]`	Setzt die lokale Subnetzmaske für den Ethernet-Port	✔	✔	✔	✔	✔	✔
`STATIC`	Öffnet das "STATISCH"-Menü	✔	✔	✔	✔	✔	✔

Siehe auch

- Menüpunkt NAT (Seite 166)

5.7.5.9 Menüpunkt CLI\BRIDGE\NAT\STATIC

NAT STATIC

Mit den Befehlen dieses Menüs legen Sie die NAT STATIC Eigenschaften fest.

CLI\BRIDGE\NAT>STATIC

Befehl	Beschreibung		Kommentar					
			IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`add <Type> <G-Port> <L-IP> <L-Port>`	Statischen NAT-Eintrag hinzufügen:		✔	✔	✔	✔	✔	✔
	Type	TCP or UDP						
	G-Port	Global Port						
	L-IP	Local IP						
	L-Port	Local Port						
`edit <Index> <E|D> [Type] [G-Port] [L-IP] [L-Port]`	Statischen NAT-Eintrag editieren:		✔	✔	✔	✔	✔	✔
	Index	Index in Tabelle						
	Type	TCP or UDP						
	G-Port	Global Port						
	L-IP	Local IP						
	L-Port	Local Port						
`delete <Index>`	Löscht einen statischen NAT Eintrag		✔	✔	✔	✔	✔	✔
`clearall`	Löscht alle statischen NAT Einträge		✔	✔	✔	✔	✔	✔

CLI\BRIDGE\NAT\STATIC>info

Index	Enabled	Type	Global Port	Local IP	Local Port
1	x	TCP	21	172.27.138.2	1026

Beispiel für die statischen Informationen

Siehe auch

- Menüpunkt NAT (Seite 166)

5.7.6 Das Menü CLI\FILTERS

5.7.6.1 Menüpunkt CLI\FILTERS\MAC1FLT

MAC Filter

Mit den Befehlen dieses Menüs legen Sie die MAC-Filter-Eigenschaften fest.

CLI\FILTERS\MAC1FLT>

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`fltmac1 <E|D>`	Aktiviert / deaktiviert den Filter.	—	—	—	—	✔	✔
`statmac1 [F|B]`	Steht dieser Wert auf F (forwarding), werden nur noch Pakete weitergeleitet, die als Quelladresse eine Adresse aus der Tabelle haben. Im Modus B (blocking) werden diese gesperrt und dafür alle anderen weitergeleitet.	—	—	—	—	✔	✔
`add <MAC-Adr.> [Beschreibung]`	Fügt eine neue Adresse zur Filterliste hinzu. Die optional angegebene Beschreibung hat keinen Einfluss auf die Liste und dient lediglich als Hilfe für den Anwender.	—	—	—	—	✔	✔
`edit <Number|MAC> [E|D] [Description]`	Ändert den angegebenen Wert.	—	—	—	—	✔	✔
`check_wds <E|D>`	Aktiviert / deaktiviert die Überprüfung auch über die WDS-Ports. In der Einstellung E werden auch die WDS-Ports überwacht.	—	—	—	—	✔	✔
`delete <Number|MAC>`	Löscht den Eintrag aus der Liste.	—	—	—	—	✔	✔
`clearall`	Löscht alle Einträge aus der Liste.	—	—	—	—	✔	✔

Siehe auch

- Menüpunkt MAC Filters (Seite 172)

5.7.6.2 Menüpunkt CLI\FILTERS\MAC2FLT

MAC-abhängige Kommunikationswege

Mit den Befehlen dieses Menüs legen Sie fest welches Gerät (MAC-Adresse) mit welchen Geräten (MAC-Adresse) kommunizieren kann.

CLI\FILTERS\MAC2FLT>

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`fltmac2 <E|D>`	Aktiviert / deaktiviert den MAC-Filter.	—	—	—	—	✔	✔
`add <SourceMAC> <DestMAC>`	Fügt einen neuen Eintrag mit Quell- und Zieladresse zum Filter hinzu.	—	—	—	—	✔	✔
`edit <Index> [E|D] [SourceMAC] [DestMAC]`	Verändert den mit Index angegebenen Eintrag. Mit [E|D] kann der Eintrag aktiviert / deaktiviert werden.	—	—	—	—	✔	✔
`delete <Index>`	Löscht den Eintrag an der angegebenen Indexposition.	—	—	—	—	✔	✔
`clearall`	Löscht alle Einträge für den MAC-Filter.	—	—	—	—	✔	✔

Siehe auch

- Menüpunkt MAC Dir Filter (Seite 172)

5.7.6.3 Menüpunkt CLI\FILTERS\PROTO

Protokollfilter

Mit den Befehlen dieses Menüs legen Sie die Protokollfilter-Eigenschaften fest.

CLI\FILTERS\PROTO>

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`clearall`	Löscht alle Einträge für den Protokoll-Filter.	—	—	—	—	✔	✔
`statprot <F|B>`	Die ausgewählten Protokolle werden weitergeleitet / nicht weitergeleitet.	—	—	—	—	✔	✔
`fltprot <E|D>`	Aktiviert / deaktiviert den Protokoll-Filter.	—	—	—	—	✔	✔
`add <Pattern> [Beschreibung]`	Fügt einen Eintrag hinzu. Beim Wert "Pattern" wird ein Wert in Hex erwartet. Als Beschreibung kann der Anwender eine kurze Notiz für dieses Protokoll angeben.	—	—	—	—	✔	✔
`edit <Index> [E|D] [Pattern] [Beschreibung]`	Ändert bzw. aktiviert / deaktiviert den Filtereintrag.	—	—	—	—	✔	✔
`delete <Index>`	Löscht den Filtereintrag.	—	—	—	—	✔	✔
`clearall`	Löscht alle Einträge aus der Tabelle.	—	—	—	—	✔	✔

Siehe auch

- Menüpunkt Protocol Filter (Seite 173)

5.7.7 Das Menü CLI\IFEATURES

5.7.7.1 Menüpunkt CLI\IFEATURES\IQOS\WLAN1 (bzw. \WLAN2 oder \WLAN3)

Hinweis

Diese Funktion ist bei der Firmwareversion 3.2 nicht verfügbar.

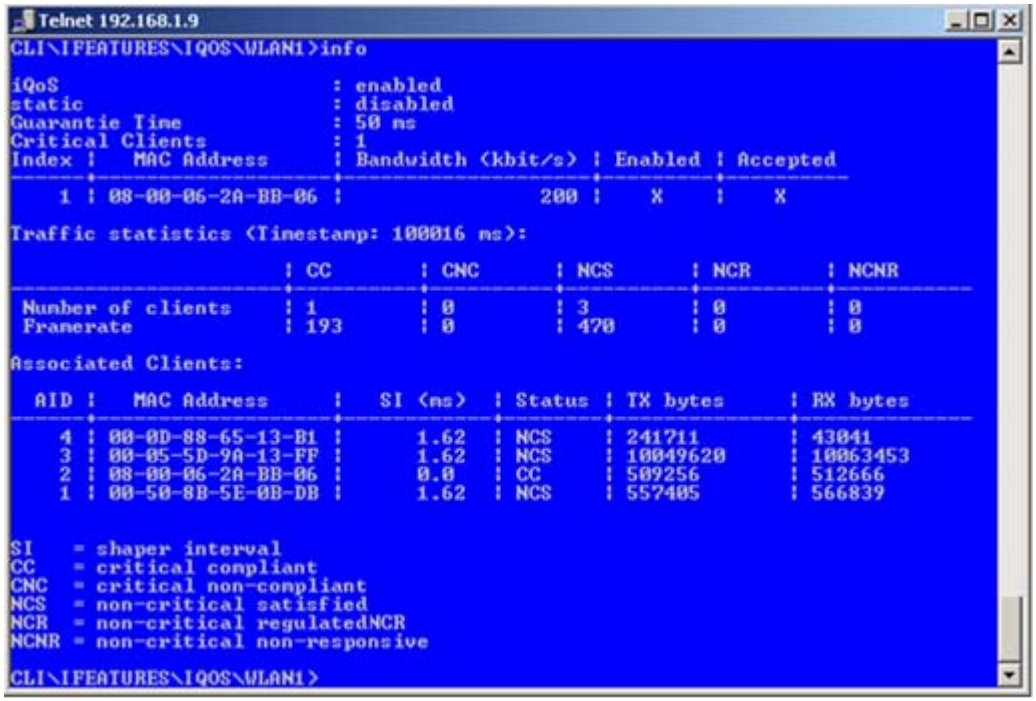
Client-spezifische Bandbreitenreservierung - Quality of Service (iQoS)

Mit den Befehlen dieses Menüs legen Sie die Eigenschaften des iQoS-Verfahrens fest bzw. liefern Informationen über iQoS.

CLI\IFEATURE\IQOS\WLAN1> (bzw. \WLAN2 oder \WLAN3)

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`iqos [E|D]`	Aktiviert / deaktiviert die iQoS-Funktionalität.	—	—	—	—	✔	✔
`static [E|D]`	Aktiviert / deaktiviert die Berechnung mit der minimalen Übertragungsrate.	—	—	—	—	✔	✔
`response [Antwortzeit]`	Legt die Antwortzeit für einen Client mit Bandbreitenreservierung fest.	15 – 1000 ms, Default 50 ms					
		—	—	—	—	✔	✔
`add <MAC> <Max_BW> [E|D]`	Anlegen eines kritischen Clients.	—	—	—	—	✔	✔
`edit <Index> <Max_BW> <E|D>`	Ändern der Einstellung eines Clients	—	—	—	—	✔	✔
`delete <Index>`	Löschen eines kritischen Client	—	—	—	—	✔	✔
`clearall`	Löschen aller kritischen Clients	—	—	—	—	✔	✔
`info`	Zeigt Informationen über iQos an.	—	—	—	—	✔	✔

Auch das CLI liefert ausführliche Informationen über iQoS. Bei dieser Ansicht wird im ersten Teil die aktuelle Konfiguration angezeigt, d.h. ob generell iQoS eingeschaltet ist, ob die Berechnungen und Reservierungen die statischen "Worst Case " Annahmen (static = enabled) bzw. die aktuelle Situation (static = disabled) zugrundelegt. Weiterhin wird die Anzahl der konfigurierten Critical Clients ausgegeben.



Für jede dieser Klassen wird in der Tabelle "Traffic statistics" angezeigt, wie viele Clients sich momentan in dem entsprechenden Zustand befinden und wie viele Pakete einer bestimmten Klasse verschickt wurden.

Die Tabelle "Associated Clients" bietet einen Überblick aller Clients, deren aktuelle Klassifikation sowie das Volumen der gesendeten und empfangenen Daten. Zusätzlich wird das Shaper Interval (SI) für jeden Client angezeigt. Das Shaper Interval ist der durch iQoS zugewiesene Mindestabstand zwischen zwei Paketen eines Clients. Für NCS-Clients wird das SI so gewählt, dass deren Bandbreite doppelt so groß wie die aktuelle Bandbreite ist.

Siehe auch

- Menüpunkt iQoS (Nur im Access Point-Modus) (Seite 174)
- Menüpunkt iQoS (Seite 188)

5.7.7.2 Menüpunkt CLI\IFEATURES\FORCED_ROAM\WLAN1 (bzw. \WLAN2 oder \WLAN3)

Zyklische Verbindungsüberwachung einer IP-Adresse

Mit den Befehlen dieses Menüs legen Sie die Eigenschaften des Forced Roaming-Verfahrens fest.

CLI\IFEATURES\FORCED_ROAM\WLAN1> (bzw. \WLAN2 oder \WLAN3)

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`froam [E|D]`	Aktiviert bzw. deaktiviert Forced Roaming on IP down.	—	—	—	—	✔	✔
`ip [IP address]`	Überwacht die Verbindung zu diesem IP-Partner.	—	—	—	—	✔	✔
`interval [100 - 5000]`	Festlegung der Überwachungszyklen zum IP-Partner in Millisekunden.	—	—	—	—	✔	✔
`lostpkts [1 - 5]`	Festlegung der maximalen Anzahl von unbeantworteten Pings, bevor das WLAN-Interface deaktiviert wird.	—	—	—	—	✔	✔

Siehe auch

- Menüpunkt Forced Roaming on IP Down (Nur im Access Point-Modus) (Seite 175)

5.7.7.3 Menüpunkt CLI\IFEATURES\LINKCHECK

Gerätebezogene Verbindungsüberwachung

Mit den Befehlen dieses Menüs legen Sie die Eigenschaften der gerätebezogenen Verbindungsüberwachung fest.

CLI\IFEATURES\LINKCHECK>

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`linkchk [E|D]`	Aktivieren / Deaktivieren der gerätebezogenen Verbindungsüberwachung.	—	—	—	—	✔	✔
`add <MAC> [Timeout]`	Fügt eine neue MAC-Adresse zur Verbindungsüberwachung mit der angegebenen Überwachungszeit hinzu. Wird keine Zeit angegeben, gilt eine Zeit von 500 ms.	—	—	—	—	✔	✔
`edit <Index|MAC> [E|D] [Timeout]`	Ändert, aktiviert oder deaktiviert einen Eintrag.	—	—	—	—	✔	✔
`delete <Index|MAC>`	Löscht den angegebenen Eintrag aus der Liste.	—	—	—	—	✔	✔
`clearall`	Löscht alle Einträge für die Verbindungsüberwachung.	—	—	—	—	✔	✔
`acknow [Index|All]`	Zeigt oder quittiert (löscht) die Link Check - Quittungsmeldungen.	Solange nicht alle Fehlermeldungen quittiert sind, bleibt der Fehler-Zustand eingeschaltet. Der Fehler-Zustand und die LED werden gelöscht, falls der Grund für den Fehler-Zustand nur eine Link Check Fehlermeldung war.					
		—	—	—	—	✔	✔

Siehe auch

- Menüpunkt Link Check (Nur im Access Point-Modus) (Seite 175)

5.7.7.4 Menüpunkt CLI\IFEATURES\REDUNDANCY

Redundante Verbindung

Mit den Befehlen dieses Menüs legen Sie die Eigenschaften der redundanten Verbindung zwischen zwei Geräten fest.

CLI\IFEATURES\REDUNDANCY>

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`redun [E|D]`	Aktiviert / deaktiviert die Redundanzfunktion	—	—	—	—	✔	✔
`wep [E|D]`	Aktiviert / deaktiviert die Verschlüsselung.	—	—	—	—	✔	✔
`mac1 <MAC-Adresse>`	Legt das Gerät fest, das redundant zur ersten Funkkarte betrieben wird.	—	—	—	—	✔	✔
`mac2 <MAC-Adresse>`	Legt das Gerät fest, das redundant zur zweiten Funkkarte betrieben wird.	—	—	—	—	✔	✔
`name [System name]`	Anstatt der MAC-Adressen kann auch der sysName des Gerätes angegeben werden.	—	—	—	—	✔	✔
`wepkey1 [Key index]`	Legt den WEP-Schlüssel des Geräts fest, das redundant zur ersten Funkkarte benutzt wird.	—	—	—	—	✔	✔
`wepkey2 [Key index]`	Legt den WEP-Schlüssel des Geräts fest, das redundant zur zweiten Funkkarte benutzt wird.	—	—	—	—	✔	✔

Siehe auch

- Menüpunkt Redundancy (Nur im Access Point-Modus) (Seite 176)

5.7.7.5 Menüpunkt CLI\IFEATURES\IP_ALIVE

Anwendungsbezogene Verbindungsüberwachung

Mit den Befehlen dieses Menüs legen Sie die Eigenschaften der anwendungsbezogenen Verbindungsüberwachung fest.

CLI\IFEATURES\IP_ALIVE>

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`ipalive <E|D>`	Aktiviert / deaktiviert die anwendungsbezogenen Verbindungsüberwachung.	—	—	—	—	✔	✔
`add <E|D> <IP-Adresse> <:Port> <Timeout>`	Fügt eine neue IP-Adresse zur Verbindungsüberwachung hinzu und aktiviert / deaktiviert die Überwachung für diese IP-Adresse.	—	—	—	—	✔	✔
`edit <Index|IP-Adr.> [:Port] [E|D] [Timeout]`	Ändert, aktiviert oder deaktiviert den über Index oder IP-Adresse angegebenen Eintrag.	—	—	—	—	✔	✔
`delete <Index|IP-Adr.`	Löscht zu überwachenden Teilnehmer.	—	—	—	—	✔	✔
`clearall`	Löscht alle Einträge für die Verbindungsüberwachung.	—	—	—	—	✔	✔
`acknow [Index|All]`	Zeigt oder quittiert (löscht) die IP-Alive Quittungsmeldungen.	Solange nicht alle Fehlermeldungen quittiert sind, bleibt der Fehler-Zustand eingeschaltet. Der Fehlerzustand und die Fault LED erlöschen, falls der einzige Grund dafür eine IP-Alive Fehlermeldung war. Der Befehl ist nicht im Client-Modus sichtbar.					
		—	—	—	—	✔	✔

Siehe auch

- Menüpunkt IP Alive (Nur im Access Point-Modus) (Seite 177)

5.7.8 Das Menü CLI\INFORM

5.7.8.1 Menüpunkt CLI\INFORM

Systemereignisse und Informationen über die Protokolle

Die Seiten dieses Menüs liefern Informationen zu Systemereignissen und Protokollen.

CLI\INFORM>

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
Info	Zeigt Informationen zum jeweiligen Menüpunkt an.	Kann in jedem Untermenü aufgerufen werden.					
		✔	✔	✔	✔	✔	✔
WLAN1	Öffnen des WLAN Menüs	✔	✔	✔	✔	—	—
ETHERNET	Öffnen des ETHERNET Menüs	—	✔	✔	✔	—	—
LOG	Öffnen des LOG Menüs	✔	✔	✔	✔	—	—
AUTHLOG	Öffnen des AUTHLOG Menüs	✔	✔	✔	✔	—	—
SIGNAL	Öffnen des Menüs Signalrekorder	✔	✔	✔	✔	—	—
spanning	Zeigt Informationen zu Spanning Tree an.	—	—	—	—	✔	✔

Siehe auch

- Menüpunkt Information (Seite 178)

5.7.8.2 Menüpunkt CLI\INFORM\LOG

Systemereignisse und Informationen über die Protokolle

Die Seiten dieses Menüs zeigen in tabellarischer Form Informationen zu Systemereignissen und Informationen über das Betriebsverhalten der Protokolle (IP, TCP, UDP, ICMP, SNMP).

CLI\INFORM\LOG>

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`events <show|clear>`	Zeigt oder löscht die Log-Tabelle.	✔	✔	✔	✔	✔	✔
`addevent <Text>`	Fügt der Log-Tabelle ein Ereignis hinzu.	✔	✔	✔	✔	✔	✔
`eventmax [Max count]`	Setzt die maximale Zahl von den Log Einträgen.	Default Wert ist 400.					
		✔	✔	✔	✔	✔	✔

Siehe auch

- Menüpunkt Log Table (Seite 178)

5.7.8.3 Menüpunkt CLI\INFORM\AUTHLOG

Protokollierung der Authentifizierung

Die Seiten dieses Menüs zeigen in tabellarischer Form Informationen zu erfolgten oder fehlgeschlagenen Authentifizierungsversuchen.

CLI\INFORM\AUTHLOG>

Befehl	Beschreibung		Kommentar					
			IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`show [0...8]`	Zeigt die Authentifizierungseinträge an. Durch Angabe eines Parameters kann die Anzeige auf bestimmte Informationen beschränkt werden:		✔	✔	✔	✔	✔	✔
	0	Alle						
	1	Good						
	2	All Errors						
	3	802.11 Errors						
	4	ACL Errors						
	5	RADIUS Errors (Request abgelehnt, Passwort abgelehnt usw.)						
	6	802.1x Errors (Timeout, keine Antwort vom RADIUS- oder WPA-Server)						
	7	Deauthenticated Errors						
	8	Deassociated Errors						
`clear`	Löscht alle Einträge.		✔	✔	✔	✔	✔	✔

Siehe auch

- Menüpunkt Auth Log (Seite 179)

5.7.8.4 Menüpunkt CLI\INFORM\WLAN1 (bzw. \WLAN2 oder \WLAN3)

Angemeldete Clients

Hier werden alle angemeldeten Clients sowie einige Zusatzinformationen (Funkkanal, Status usw.) angezeigt.

CLI\INFORM\WLANx>

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`station`	Zeigt Informationen über die verbundenen Stationen an.	✔	✔	✔	✔	✔	✔
`resetStats`	Setzt die Statistiken zurück, die mit dem Befehl Station angezeigt werden.	✔	✔	✔	✔	✔	✔
`apinfo`	Zeigt Informationen über den Access Point an.	(nur im Access Point-Modus)					
		—	—	—	—	✔	✔
`scan`	Zeigt alle Access Points in der Umgebung an. Nur möglich, wenn iPCF ausgeschaltet ist.	✔	✔	✔	✔	✔	✔
`noise`	Zeigt Störungen auf den einzelnen Kanälen an.	✔	✔	✔	✔	✔	✔
`stasort`	Zeigt Informationen über die verfügbaren Access Points an, sortiert nach MAC Adressen oder Signalstärke.	✔	✔	✔	✔	—	—
`scanww`	Zeigt alle Access Points ohne Berücksichtigung des Country Code an.	—	✔	✔	✔	✔	✔
`vap`	Zeigt alle konfigurierten SSIDs (VAPs) an.	—	—	—	—	✔	✔
`overlap`	Zeigt die Accesspoints auf dem eingestellten oder auf benachbarten Kanälen.	—	—	—	—	✔	✔
`over_age [1..7200]`	Ändert das Aging-Interval (in Minuten) für die Liste der benachbarten Access Points. Ist ein AP länger als die hier eingestellte Zeit inaktiv wird er aus der Liste entfernt.	—	—	—	—	✔	✔

Siehe auch

- Menüpunkt Client List (Seite 181)

5.7.8.5 Menüpunkt CLI\INFORM\SIGNAL

Anzeigen der aktuellen Signalstärke und Aufzeichnen einer Messreihe

Mit den Befehlen dieses Menüs legen Sie die Eigenschaften des Signal Rekorders fest.

CLI\INFORM\SIGNAL>

Befehl	Beschreibung	Kommentar					
		IWLAN/ PB LINK	W744	W746	W747	W78x	W78x RR
`recstart <Intervall> [Anzahl. Aufzeichn.-Punkte]`	Startet die Signal Aufzeichnung. Das Intervall, in dem das aktuelle Signal aufgezeichnet wird, kann zwischen 1 und 1000 Millisekunden betragen. Für die Anzahl der Aufzeichnungs¬punkte ist ein Wert zwischen 1 und 20000 möglich.	Dieser Befehl ist nur im Client-Modus verfügbar.					
		✔	✔	✔	✔	✔	✔
`recstop`	Beendet die Signalaufzeichnung vorzeitig.	Dieser Befehl ist nur im Client-Modus verfügbar.					
		✔	✔	✔	✔	✔	✔
`dispstart [Intervall]`	Gibt die aktuelle Signalstärke zyklisch auf dem CLI aus. Die Intervalllänge kann zwischen 100 und 10000 Millisekunden betragen	Dieser Befehl ist nur im Client-Modus verfügbar.					
		✔	✔	✔	✔	✔	✔
`dispstop`	Beendet die zyklische Ausgabe der Signalstärke.	Dieser Befehl ist nur im Client-Modus verfügbar.					
		✔	✔	✔	✔	✔	✔
`exit`	Beendet die CLI/TELNET Verbindung	Dieser Befehl ist nur im Client-Modus verfügbar					
		✔	✔	✔	✔	✔	✔
`info`	Zeigt die Parameter des Signalrekorders	Dieser Befehl ist nur im Client-Modus verfügbar					
		✔	✔	✔	✔	✔	✔

Siehe auch

- Menüpunkt Signal Recorder (Seite 191)

5.8 Konfiguration mit dem PRESET-PLUG

5.8.1 Funktionsprinzip des PRESET-PLUG

Mehrfachverwendung von Konfigurationsdaten

Mit dem PRESET-PLUG können Sie mehrere, gleich konfigurierte SCALANCE W786 auf einfachste Weise mit einer Konfiguration versehen. Sie übertragen mit dem PRESET-PLUG eine bestehende Konfiguration auf beliebig viele andere Geräte. Dieses Vorgehen ist besonders bei der Inbetriebnahme vieler gleich parametrierter WLAN-Clients vorteilhaft, weil nicht jeder Client manuell parametriert werden muss.

Hinweis

Um eine Verdopplung von IP-Adressen zu vermeiden, werden die IP Parameter durch Anwenden des PRESET-PLUGs nicht verändert, sondern bleiben erhalten.

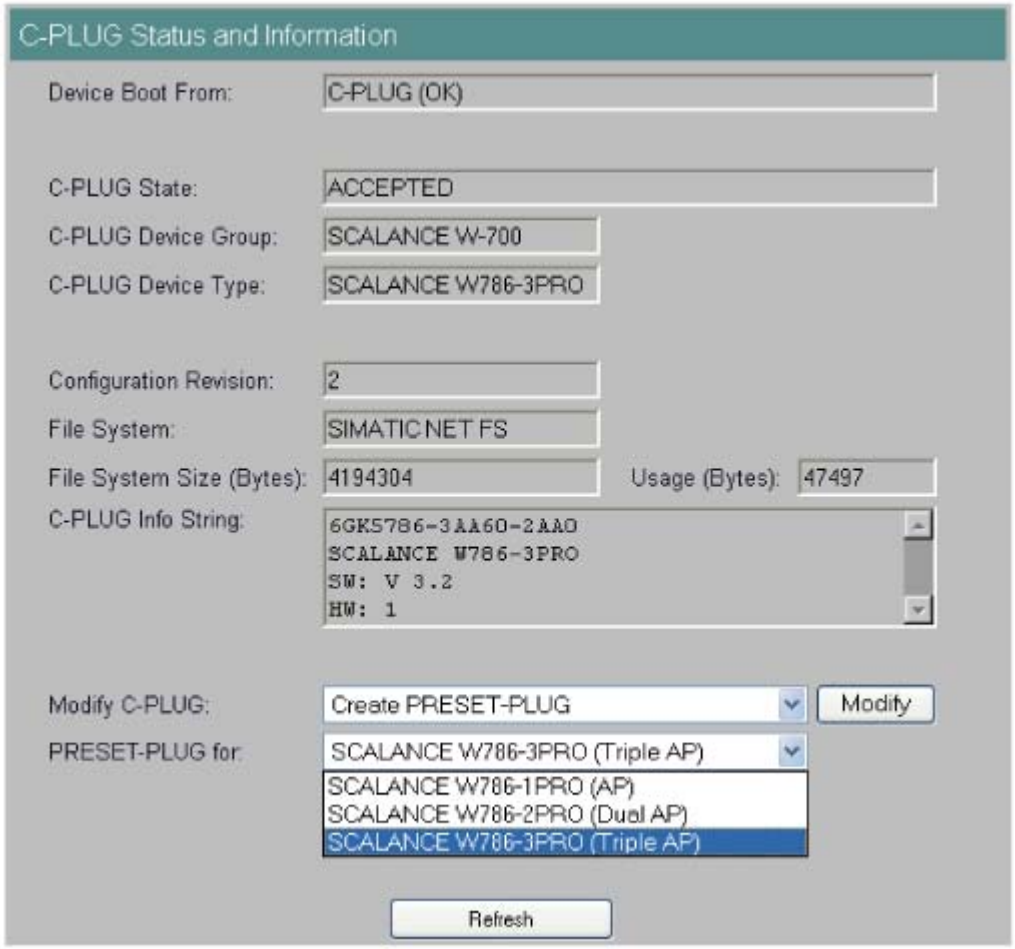
Ist der PRESET-PLUG gesteckt, wird das WLAN Interface des Geräts deaktiviert. Der WLAN Betrieb mit gestecktem PRESET-PLUG ist nicht möglich.

5.8.2 Erstellen einer Konfiguration mit einem neuen PRESET-PLUG

Vorgehensweise

Führen Sie folgende Schritte durch, um einen PRESET-PLUG mit einer Konfiguration zu versehen:

1. Stecken Sie den PRESET-PLUG in den C-PLUG-Steckplatz eines ausgeschalteten Geräts mit der gewünschten Konfiguration und schalten Sie das Gerät ein.
2. Starten Sie das Web Based Management und wählen Sie das Menü **System > C-PLUG**.
3. Wählen Sie in der Klappliste "Modify C-PLUG" den Eintrag "Create PRESET-PLUG".



4. Legen Sie im Feld "PRESET PLUG for" fest, für welches Gerät der PRESET-PLUG erstellt werden soll. Der so erstellte PRESET-PLUG funktioniert nur bei dem von Ihnen gewählten Gerätetyp. Die vorangegangene Abbildung zeigt als Beispiel die Auswahlmöglichkeiten bei einem SCALANCE W786.
5. Klicken Sie die Schaltfläche "Modify", um die Konfiguration des Geräts auf den PRESET-PLUG zu übertragen.
6. Schalten Sie das Gerät aus und entnehmen Sie den PRESET-PLUG.

5.8.3 Ändern eines PRESET-PLUG, der bereits Konfigurationsdaten enthält

Vorgehensweise

Führen Sie folgende Schritte durch, um die Konfigurationsdaten auf einem PRESET-PLUG zu ändern:

1. Stecken Sie den PRESET-PLUG in den C-PLUG Steckplatz eines ausgeschalteten SCALANCE W-700 und schalten Sie das Gerät ein. Die LEDs P1 und R1 blinken gelb, um zu signalisieren, dass der PRESET-PLUG erkannt wurde.
2. Starten Sie das Web Based Management; dort werden die aktuellen Einstellungen des PRESET-PLUGs angezeigt.
3. Nehmen Sie die gewünschten Änderungen der Konfiguration vor.
4. Wählen Sie in der Klappliste "Modify C-PLUG" den Eintrag "Create PRESET-PLUG".
5. Legen Sie im Feld "PRESET PLUG for" fest, für welches Gerät der PRESET-PLUG erstellt werden soll.
6. Klicken Sie die Schaltfläche "Modify", um die Konfiguration des Gerätes auf den PRESET-PLUG zu übertragen.
7. Schalten Sie das Gerät aus und entnehmen Sie den PRESET-PLUG.

5.8.4 Inbetriebnahme eines Geräts mit einem PRESET-PLUG

Vorgehensweise

Hinweis

Für die einwandfreie Funktion muss der PRESET-PLUG einen für das Zielgerät passenden Inhalt haben.

Führen Sie folgende Schritte durch, um die Inbetriebnahme eines Gerätes mit den Konfigurationsdaten auf einem PRESET-PLUG durchzuführen:

1. Stecken Sie den PRESET-PLUG in den C-PLUG Steckplatz des Gerätes, das Sie mit einer Konfiguration versehen wollen.
2. Schalten Sie das Gerät ein. Die LEDs "P1" und "R1" (sowie "Rx" bei einem SCALANCE W-700 mit mehr als einer Funkschnittstellen) blinken gelb, um zu signalisieren, dass der PRESET-PLUG erkannt wurde.
3. Drücken Sie den Reset-Taster neben dem C-PLUG-Steckplatz kurz, um die Voreinstellungen des PRESET-PLUG im Gerät zu speichern.
4. Wenn alle Daten vom PRESET-PLUG auf das Gerät übertragen wurden, ändern sich die LEDs von Blinklicht auf Dauerlicht.
5. Schalten Sie das Gerät aus und entnehmen Sie den PRESET-PLUG.

Hinweis

Beim nächsten Anlauf startet das Gerät mit den PRESET-PLUG Einstellungen und der vorherigen IP-Konfiguration.

Instandhalten und Warten

6

6.1 Laden einer neuen Firmware über FTP

Vorgehen

Über FTP können Sie einen SCALANCE W-700 auch dann mit einer neuen Firmware versehen, wenn das Gerät nicht über das WEB Based Management oder das CLI erreichbar ist. Das kann der Fall sein, wenn es während eines Firmware-Updates zu einem Spannungsausfall gekommen ist. Führen Sie folgende Schritte durch, um eine neue Firmware über FTP zu laden:

1. Schalten Sie das Gerät spannungslos.
2. Drücken Sie nun den Reset-Taster und schließen Sie das Gerät mit gedrücktem Taster wieder an die Versorgungsspannung an.
3. Halten Sie den Taster so lange gedrückt, bis die rote Fehler LED (F) nach ca. 2 Sekunden anfängt zu blinken.
4. Lassen Sie nun den Taster los. Der Bootloader wartet in diesem Zustand auf eine neue Firmware-Datei, die Sie per FTP laden können.
5. Verbinden Sie einen PC über die Ethernet-Schnittstelle mit dem SCALANCE W-700.
6. Vergeben Sie mit dem Primary Setup Tool eine IP-Adresse für den SCALANCE W-700.
7. Wechseln Sie in einer DOS-Box in das Verzeichnis, in dem sich die Datei mit der neuen Firmware befindet und rufen Sie danach das Kommando "ftp <ip-adresse>" auf. Alternativ dazu können Sie einen anderen FTP-Client verwenden.
8. Geben Sie als Login und Passwort jeweils "siemens" ein.
9. Laden Sie die neue Firmware mit dem Kommando "put <firmware>".
10. Nachdem die Firmware komplett auf das Gerät übertragen ist, wird das Gerät automatisch neu gestartet.

6.2 Wiederherstellen der Default-Parameter

Vorgehen

Führen Sie folgende Schritte durch, um die Gerätparameter auf die Werkseinstellungen zurückzusetzen:

ACHTUNG
Beim Zurücksetzen der Geräteparameter gehen alle bisher vorgenommenen Einstellungen verloren!

1. Schalten Sie das Gerät spannungslos.
2. Drücken Sie nun den Reset-Taster und schließen Sie das Gerät mit gedrücktem Taster wieder an die Versorgungsspannung an.
3. Halten Sie den Taster so lange gedrückt, bis die rote Fehler LED (F) nach ca. 10 Sekunden aufhört zu blinken und in Dauerlicht wechselt.
4. Lassen Sie nun den Taster los und warten Sie, bis die Fehler-LED (F) wieder erlischt.
5. Das Gerät startet dann automatisch mit den Default Parametern.

Technische Daten

7

7.1 Technische Daten SCALANCE W786

Produktvarianten

- SCALANCE W786-1PRO mit einem Funkinterface und in den Varianten mit zwei internen Antennen oder zwei externen Antennenanschlüssen und mit RJ45 oder LWL-Anschluss
- SCALANCE W786-2PRO mit zwei Funkinterfaces und in den Varianten mit vier internen Antennen oder vier externen Antennenanschlüssen und mit RJ45 oder LWL-Anschluss
- SCALANCE W786-3PRO mit drei Funkinterfaces und in den Varianten mit sechs externen Antennenanschlüssen und mit RJ45 oder LWL-Anschluss

Datenübertragung

Übertragungsrate Ethernet	10/100 Mbit/s
Übertragungsrate Funk	1 ... 54 Mbit/s (108 Mbit/s)
Unterstützte Standards Funk	802.11a 802.11b 802.11g 802.11h
Unterstützte Standards Energieversorgung	802.3af (Power over Ethernet)

Schnittstellen

Energie	• Einspeisung DC 48 V über mitgelieferten Anschlussstecker • RJ45-Buchse Power over Ethernet (DC 48 V) • 2 Einspeisungen DC 12 - 24 V mit optionalem Stromversorgungsadapter (als Zubehör erhältlich) • AC 110 - 230 V mit optionalem Stromversorgungsadapter (als Zubehör erhältlich) Stromversorgung galvanisch trennend ausgeführt entsprechend IEEE 802.3af, Isolationswiderstand > 2MOhm.

Daten	• RJ45-Buchse für Ethernet oder bei Geräten für Lichtwellenleiter: 1 x 2 BFOC-Buchsen • Ausführungsabhängig bis zu sechs R-SMA-Antennenbuchsen

Elektrische Daten

Leistungsaufnahme abhängig von der Einspeisung	PoE	12,9 W
	DC 48 V	12,9 W
	DC 12 - 24 V (Adapter)	15 W
	AC 110 - 230 V (Adapter)	15 W

Konstruktiver Aufbau

Abmessungen (B x H x T)	251 mm x 251 mm x 72 mm	
Gewicht (Ausführung mit drei IWLAN-Schnittstellen)	Ohne Stromversorgungs-adapter	2241 g
	Mit Stromversorgungs-adapter DC 12 - 24 V	2428 g
	Mit Stromversorgungs-adapter AC 110 - 230 V	2433 g

Zulässige Umgebungsbedingungen

Betriebstemperatur	-40°C ... 70°C
Transport- und Lagertemperatur	-40°C ... 85°C
Schutzart	geprüft nach IP65

MTBF Angaben (mean time between failure)

MTBF	61 Jahre

Spezifikationen und Bestell-Nummern

Typ	Anzahl der WLAN-Schnittstellen	Anzahl und Art der Ethernet-Schnittstellen	Anzahl interne Antennen	Anzahl R-SMA-Buchsen für externe Antennen	Bestell-Nr.
W786-1PRO	1	1 RJ45	1 (Diversity(2))	—	6GK5786-1BA60-2AA0 6GK5786-1BA60-2AB0 (1)
W786-1PRO	1	1 RJ45	—	2	6GK5786-1AA60-2AA0 6GK5786-1AA60-2AB0 (1)
W786-1PRO	1	1 ST Duplex Multimode Lichtwellen-leiter	1 (Diversity(2))	—	6GK5786-1BB60-2AA0 6GK5786-1BB60-2AB0 (1)
W786-1PRO	1	1 ST Duplex Multimode Lichtwellen-leiter	—	2	6GK5786-1AB60-2AA0 6GK5786-1AB60-2AB0 (1)
W786-2PRO	2	1 RJ45	2 (Diversity(2))	—	6GK5786-2BA60-2AA0 6GK5786-2BA60-2AB0 (1)
W786-2PRO	2	1 RJ45	—	4	6GK5786-2AA60-2AA0 6GK5786-2AA60-2AB0 (1)
W786-2PRO	2	1 ST Duplex Multimode Lichtwellenleiter	2 (Diversity(2))	—	6GK5786-2BB60-2AA0 6GK5786-2BB60-2AB0 (1)
W786-2PRO	2	1 ST Duplex Multimode Lichtwellen-leiter	—	4	6GK5786-2AB60-2AA0 6GK5786-2AB60-2AB0 (1)
W786-3PRO	3	1 RJ45	—	6	6GK5786-3AA60-2AA0 6GK5786-3AA60-2AB0 (1)

Typ	Anzahl der WLAN-Schnittstellen	Anzahl und Art der Ethernet-Schnittstellen	Anzahl interne Antennen	Anzahl R-SMA-Buchsen für externe Antennen	Bestell-Nr.
W786-3PRO	3	1 ST Duplex Mulitmode Lichtwellen-leiter	—	6	6GK5786-3AB60-2AA0 6GK5786-3AB60-2AB0 (1)

(1) US-Variante

(2) Pro WLAN-Schnittstelle gibt es zwei interne Antennen. Es wird immer die verwendet, die die bestmögliche Datenübertragung gewährleistet (Diversity).

Anhang

A

A.1 Private MIB-Variablen des SCALANCE W78x / W74x

Download der MIB des SCALANCE W-700 über den Internet Explorer

Über die URL
`http://<IP-Adresse>/snScalanceW.mib`
kommen Sie, falls noch nicht angemeldet, zum Login Fenster. Nach erfolgter Anmeldung gelangen Sie zur Private-Mib des SCALANCE W-700. Zum Speichern auf Ihrem PC sollte die Quelltextansicht aktiviert sein.

OID

Die Private MIB-Variablen des SCALANCE W78x haben folgenden Object Identifier:

```
iso(1).org(3).dod(6).internet(1).private(4).
  enterprises(1).ad(4196).adProductMibs(1).simaticNet(1).
  iScalanceW(4)
```

Variablen für Access Points und Clients

Die folgende Tabelle zeigt die Private MIB-Variablen die bei Access Points und Clients zur Verfügung stehen:

Name	OID	Beschreibung	Anzahl der Objekte
snDownload	1.3.6.1.4.1.4196.1.1.4.100.1.5	Donwload Information und Kontrollvariablen für Image, Konfigurationsdatei, Eventstabelle.	17
snNvLog	1.3.6.1.4.1.4196.1.1.4.100.1.6	Protokoll für Ereignisse.	8
snTrapInfo	1.3.6.1.4.1.4196.1.1.4.100.1.7	Informationen über Traps.	6
snGen	1.3.6.1.4.1.4196.1.1.4.100.1.8	Allgemeine Information, die nicht MIB-2-konform ist.	23
snTcpip	1.3.6.1.4.1.4196.1.1.4.100.1.10	IP address, Subnet Mask, Default Gateway, DHCP Status…	5
snScalanceWCommon	1.3.6.1.4.1.4196.1.1.4.100.2.1	SCALANCE W-700 - spezifische Einstellungen.	24
snScalanceWFilter	1.3.6.1.4.1.4196.1.1.4.100.2.4	Protokollfilter- und Stormthreshold-Einstellungen	18
snScalanceWStats	1.3.6.1.4.1.4196.1.1.4.100.2.5	Information über WLAN 1 und WLAN 2 Schnittstellen.	62

Name	OID	Beschreibung	Anzahl der Objekte
snScalanceWDevices	1.3.6.1.4.1.4196.1.1.4.100.2.6	AP Mode: Liste und Informationen aller Clients, die momentan "associated" oder angeschlossen sind. Client Mode: Liste der Geräte, mit denen der Client momentan verbunden ist.	49
snScalanceWScan	1.3.6.1.4.1.4196.1.1.4.100.2.7	Client Mode: Liste der erreichbaren WLANs und Information, ob sich die Clients mit diesen verbinden können.	11
snScalanceWAccess	1.3.6.1.4.1.4196.1.1.4.100.2.9	Liste der IP-Adressen, die auf die Managementschnittstelle zugreifen dürfen.	5

Variablen, die nur bei Access Points zur Verfügung stehen

Name	OID	Beschreibung	Anzahl der Objekte
snScalanceWAcl	1.3.6.1.4.1.4196.1.1.4.100.2.8	Informationen und Einstellungen zu den Access Control Listen.	9
snScalanceWVirtualAp	1.3.6.1.4.1.4196.1.1.4.100.2.10	Informationen zu den derzeit konfigurierten virtuellen APs.	17

Traps für Access Points und Clients

Name	Specific Index	Variable	Beschreibung
snScalanceWPowerLineDown	32	snScalanceWChangedPowerLine - The power line where the last Power-Down occurred. 1-M12, 2-Ethernet Power	Wird bei einem Spannungsausfall an M12- oder Ethernet Spannungs-Anschluss generiert.
snScalanceWPowerLineUp	32	snScalanceWChangedPowerLine - The power line where the last Power-Up occurred. 1-M12, 2-Ethernet Power	Wird beim Einschalten der Spannung an M12-oder Ethernet Spannungs-Anschluss generiert.
snScalanceWFault	41	snScalanceWFaultValue - Fault value: 0 = no fault, bit 0 = power M12 is off, bit 1 = linkdown, bit 2 = internal error, bit 23 = Link Check error, bit 24 = IP Alive broken, bit 25 = power ethernet is off, bit 26 = Cold/Warm start, bit 27 = C-PLUG error, bit 28 = iQoS error, bit 29 = Redundancy error"	Wird generiert, falls die Variable snScalanceWFaultValue geändert wird. Das Bit wird entsprechend dem aufgetretenen Ereignis auf "1" gesetzt.

Name	Specific Index	Variable	Beschreibung
snScalanceWIQOS	51	snScalanceWIQOSValue - Description of the last snScalanceWIQOS Trap	
snScalanceWLinkCheckOff	81	snScalanceWLinkCheckValue - Description of the last snScalanceWLinkCheckOff Trap	Wird im Falle eines Timeouts bei einem mit LinkCheck überwachten Client generiert.
snScalanceWLinkIntegrityOn	82	snScalanceWLinkCheckValue - Description of the last snScalanceWLinkCheckOn Trap	Wird generiert, falls ein über Link Check überwachter Client sich nach einem Timeout wieder am AP anmeldet.
snScalanceWClientAuthenticated	85	SnScalanceWClientsIndex - An index of the client in snScalanceWClients table	Wird generiert, wenn sich ein Client am AP anmeldet.
snScalanceWClientDeAuthenticated	86	SnScalanceWClientsIndex - An index of the client in snScalanceWClients table	Wird generiert, wenn sich ein Client vom AP abmeldet.
snScalanceWRedundancy	53	SnScalanceWRedundancyValue- Description of the last Redundancy Trap. SnScalanceWRedundancyState- Status of redundancy connection	Wird generiert, falls sich der Zustand der redundanten Verbindung ändert, z.B. wenn die Verbindung vom Wireless Interface A abbricht.

Traps, die nur bei Access Points zur Verfügung stehen

Name	Specific Index	Variable	Beschreibung
snScalanceWOverlapAP	101	snScalanceWOverlapAPValue - Description of the last OverlapAP Trap.	Wird generiert, wenn ein Access Point auf dem eigenen oder einem überlappenden Funkkanal entdeckt wird.
snScalanceWiPCFPNIOmaxSTAs	111	snScalanceWPNIOValue - Description of the last snScalanceWiPCFPNIOmaxSTAs or snScalanceWiPCFPNIOCycleTime Trap	Wird generiert, wenn für die angegebene Update Time im iPCF-Modus mit PNIO Support zu viele Clients angemeldet sind.
snScalanceWiPCFPNIOCycleTime	112	snScalanceWPNIOValue - Description of the last snScalanceWiPCFPNIOmaxSTAs or snScalanceWiPCFPNIOCycleTime Trap	Wird generiert, wenn die angegeben Update Time im iPCF-Modus mit PNIO-Support nicht eingehalten werden kann.

Name	Specific Index	Variable	Beschreibung
snScalanceWForcedRoamingVapStateChanged	121	snScalanceWVirtualApIndex - Index of the VAP snScalanceWVirtualApState - Current State of the VAP unknown (0) authenticated (1) associated (2) powersafe (3) adhoc (4) joined (5) vap-is-up (6) vap-starting (7) vap-is-down (8) locked (9) vap-connected (10)	Wird generiert, wenn sich der Status des VAPs ändert.

A.2 Auslegung und Berechnung von Funksystemen (Beispiel RCoax)

Dezibel als logarithmische Maßeinheit

In der Funktechnik erfolgen Berechnungen meistens in Dezibel (dB). Unter Dezibel versteht man den Logarithmus eines Verhältniswerts. Mathematisch formuliert kann dies mit folgender Gleichung wiedergegeben werden:

Dezibelwert = 10 * log (Verhältniswert)

Für eine Beispielrechnung ergeben sich dann folgende Dezibelwerte:

Verhältniswert	Dezibelwert
0,001	-30 dB
0,1	-10 dB
0,2	-7 dB
0,4	-4 dB
0,5	-3 dB
1	0 dB
2	3 dB
4	6 dB

Wie aus dem Beispiel erkennbar ist, hat die Halbierung eines Werts die Verminderung des Dezibelwerts um 3 dB zur Folge. Dieser Sachverhalt gilt unabhängig von der gewählten Bezugsgröße, weil nur der Verhältniswert maßgeblich ist. Welche Bezugsgröße zugrunde gelegt wird, ist aus den zusätzlichen Buchstaben bzw. Zahlen hinter der Dimension dB ersichtlich. In der Akustik beispielsweise ist für einen Wert in dB(A) die Hörschwelle die Bezugsgröße.

Leistungsangaben in dBm

Eine gebräuchliche Bezugsgröße in der Funktechnik ist eine Leistung von 1mW. Leistungen können damit in der Einheit Dezibel Milliwatt (dBm) angegeben werde. Es gilt folgende Umrechnungsformel:

P [dBm] = 10 * log (P [mW] / 1 mW)

Damit ergeben sich folgende Leistungsangaben in dBm:

Leistungswert		Dezibelwert
0,5 mW	≈	-3 dBm
1 mW	≈	0 dBm
2 mW	≈	3 dBm
4 mW	≈	6 dBm
10 mW	≈	10 dBm
100 mW	≈	20 dBm
200 mW	≈	23 dBm
1000 mW	≈	30 dBm

Mit Leistungsangaben können sehr einfach Verstärkungen und Dämpfungen berechnet werden. Zur Berechnung eines Gesamtsystems müssen lediglich die logarithmischen Einzelwerte für Verstärkung und Dämpfung addiert werden.

Sendeleistungen in dBm

Die Angaben in den folgenden Tabellen gelten für folgende SIMATIC NET-Produkte:

- Access Point SCALANCE W786-1PRO
- Access Point SCALANCE W786-2PRO
- Access Point SCALANCE W786-3PRO

Tabelle A-1 Sendeleistung im IEEE 802.11b-Modus (2,4 GHz)

Datenrate [Mb/s]	P_0 [dBm]
1	20
2	20
5,5	20
11	20

Tabelle A-2 Sendeleistung im IEEE 802.11g-Modus (2,4 GHz)

Datenrate [Mb/s]	P_0 [dBm]
6	20
9	20
12	20
18	20
24	20
36	20
48	20
54	19

Tabelle A-3 Sendeleistung im IEEE 802.11a/h-Modus (5 GHz)

Datenrate [Mb/s]	P_0 [dBm]
6	20
9	20
12	20
18	20
24	20
36	20
48	20
54	19

Leistungsangaben in dBi

Bei Leistungsangaben in dBi ist die Bezugsgröße die Sendeleistung des isotropen Kugelstrahlers. Eine solche (nur theoretisch mögliche) Antenne strahlt die Energie von einem punktförmigen Zentrum gleichmäßig in alle Richtungen.

Aus der gerichteten Abstrahlung einer realen Antenne ergibt sich dann der dBi-Wert als sogenannter Antennengewinn. Dieser Begriff ist insofern missverständlich, als durch eine Antenne keine Energie im physikalischen Sinn gewonnen wird. Die höhere Abstrahlung einer passiven Antenne ergibt sich allein durch die Konzentration der Abstrahlung in eine bestimmte Richtung. In anderen Raumsegmenten ist entsprechend weniger Leistung vorhanden.

Verluste durch Längsdämpfung

Die Längsdämpfung der Leckwellenleitung ist abhängig von seiner Länge und berechnet sich nach folgender Formel:

$a_{rc} = \alpha_{rc} * l$

a_{rc} Längsdämpfung des Kabels in dB

α_{rc} Dämpfungskoeffizient in dB/m wie in den technischen Daten des Kabels angegeben:
RCoax-Leitung: 0,17 dB/m bei 2,4 GHz
Verbindungsleitung: 0,55 dB/m bei 2,4 GHz

l Gesamtlänge der Leitung in m

Verluste durch Kopplungsdämpfung

Die Kopplungsdämpfung cd berücksichtigt die Verluste beim Übergang vom Kabel in den umgebenden Raum. Die Kopplungsdämpfung hängt von der Bauform des Kabels und seinen physikalischen Eigenschaften ab. Werte für die Kopplungsdämpfung sind deshalb in den technischen Daten des jeweiligen Kabels angegeben.

Verluste durch Freiraumdämpfung

Die Freiraumdämpfung afr gibt an, welche Dämpfung zwischen RCoax-Leitung und Kommunikationspartner vorhanden ist. Maßgeblich ist hier also die Entfernung zwischen RCoax-Leitung und Kommunikationspartner. Es gilt folgende Formel:

$a_{fr} = 20 * \log(4\pi d / \lambda)$

a_{fr} Freiraumdämpfung in dB.

d Abstand zwischen Kabel und Antenne in m.

λ Wellenlänge der elektromagnetischen Schwingung in m, bei einer Frequenz von 2,4 GHz ist die Wellenlänge 0,125 m.

Hinweis

Die genannte Formel ist nur für die RCoax-Leitung bei 2,4 GHz gültig.

IEC 61196-4

Werte für die Kopplungsdämpfung nach IEC 61196-4 beinhalten bereits eine Freiraumdämpfung von 2 m. Für die Berechnung der tatsächlichen Kopplungsdämpfung muss deshalb von diesem Wert eine Freiraumdämpfung für den Abstand 2 m abgezogen werden. Die Kopplungsdämpfung für einen vorgegebenen Abstand zwischen RCoax-Leitung und der Antenne des Kommunikationspartners wird also nach folgender Formel berechnet:

$c_d = c_{95} - 20 * \log(4\pi * 2m / \lambda) + 20 * \log(4\pi d / \lambda)$

cd Kopplungsdämpfung des Kabels in dB für einen vorgegebenen Abstand zwischen Kabel und Antenne.

c_{95} c_{95}-Wert der Kopplungsdämpfung (Angaben im Datenblatt des Kabels)

λ Wellenlänge der elektromagnetischen Schwingung in m. Bei einer Frequenz von 2,4 GHz ist die Wellenlänge 0,125 m.

d Abstand zwischen Kabel und Antenne in m.

Für eine Frequenz von 2,4 GHz können Sie auch mit folgender Zahlenwertgleichung rechnen, wobei Sie den Abstand d in Metern angeben müssen:

$c_{d\ 2,4\ GHz} = c_{95} - 46\ dB + 20 * \log(100 * d)$

Damit ergeben sich beispielsweise für ein SIEMENS SIMATIC NET IWLAN RCoax Cable PE 1/2" 2,4 GHz (c_{95} = 69 dB bei 2,4 GHz) folgende Kopplungsdämpfungen:

Abstand	Kopplungsdämpfung
1 m	63 dB
2 m	69 dB
5 m	77 dB
10 m	83 dB
100 m	103 dB

Hinweis

Die genannte Formel ist nur für die RCoax-Leitung bei 2,4 GHz gültig.

Verluste durch Leistungsteiler

Typischerweise muss für einen Zweifach-Leistungsteiler (ein Eingang, zwei Ausgänge z.B. RCoax N-Connect Female Power Splitter 2-Way) ein Verlust von **3 dB** berücksichtigt werde.

Empfängerempfindlichkeit

Die Empfängerempfindlichkeit ist die Leistung, die einem Empfänger mindestens zugeführt werden muss, damit Kommunikation stattfinden kann. Die Empfängerempfindlichkeit ist eine gerätespezifische Eigenschaft und hängt vom Übertragungsverfahren und der Datenrate ab. Die Angaben in den folgenden Tabellen gelten für folgende SIMATIC NET-Produkte:

- Access Point SCALANCE W786-1PRO
- Access Point SCALANCE W786-2PRO
- Access Point SCALANCE W786-3PRO

Tabelle A-4 Empfängerempfindlichkeit im IEEE 802.11b-Modus (2,4 GHz)

Datenrate [Mb/s]	P_e [dBm]
1	-97
2	-93
5,5	-92
11	-88

Tabelle A-5 Empfängerempfindlichkeit im IEEE 802.11g-Modus (2,4 GHz)

Datenrate [Mb/s]	P_e [dBm]
6	-91
9	-90
12	-89
18	-87
24	-84
36	-80
48	-76
54	-74

Tabelle A-6 Empfängerempfindlichkeit im IEEE 802.11a/h-Modus (5 GHz)

Datenrate [Mb/s]	P_e [dBm]
6	-91
9	-90
12	-90
18	-88
24	-85
36	-82
48	-76
54	-72
72 [*]	-76

Datenrate [Mb/s]	P_e [dBm]
96 [*]	-71
108 [*]	-68

[*] Turbo Mode

Systemberechnung am Beispiel RCoax

Die Berechnung des Gesamtsystems zeigt, ob mit den gewünschten Komponenten eine Kommunikation mit der gewünschten Übertragungsrate möglich ist. Dazu werden von der Sendeleistung alle Verluste (Längsdämpfung, Freiraumdämpfung, Leistungsteiler usw.) abgezogen. Ein Antennengewinn wird addiert. Das Ergebnis ist die Leistung, die einem Empfänger zugeführt wird. Diese Leistung muss größer sein als die Empfängerempfindlichkeit. Die Berechnung kann mit folgender Formel durchgeführt werden:

$P_e = P_0 - a_{rc} - c_d - a_{ps} + G_{ANT} - \Delta_{rc} - \Delta_{fr} > P_{e\,min}$

P_e Empfängereingangsleistung in dBm

P_0 Sendeleistung in dBm

a_{rc} Längsdämpfung der RCoax-Leitung und der Zuleitung in dB

c_d Kopplungsdämpfung für den Abstand zwischen RCoax-Leitung und Kommunikationspartner

a_{ps} Leistungsteilerverluste in dB

G_{ANT} Antennengewinn in dB

Δ_{rc} Korrekturwert für die Längsdämpfung in dB. Abhängig von den konkreten Betriebsbedingungen zwischen 5 und 15 dB.

Δ_{fr} Korrekturwert für die Freiraumdämpfung in dB. Abhängig von den konkreten Betriebsbedingungen zwischen 0 und 20 dB.

$P_{e\,min}$ Empfängerempfindlichkeit in dBm

Glossar

Access Point

Ein (**W**ireless) **A**ccess **P**oint (WAP, engl. "drahtloser Zugangsknoten") ist ein elektronisches Gerät, das als Schnittstelle zwischen einem Mobilfunknetz und einem kabelgebundenen Rechnernetz fungiert. Endgeräte (Clients) stellen über einen Wireless Adapter eine Funkverbindung zum Wireless Access Point her, der wiederum über ein Kabel mit einem fest installierten Kommunikationsnetz verbunden ist.

ACL

Access Control List. Liste mit MAC-Adressen, die zum Zugriff auf das Mobilfunknetz berechtigt sind.

Ad-Hoc-Netz

Mobilfunknetz zwischen einzelnen Geräten (Point-to-point).

AES

Advanced **E**ncryption **S**tandard, Verschlüsselung nach dem Rijndael-Algorithmus.

Anlage

Gesamtheit aller elektrischen Betriebsmittel. Zu einer Anlage gehören u.a.: Speicherprogrammierbare Steuerung, Geräte für Bedienen und Beobachten, Bussysteme, Feldgeräte, Antriebe, Versorgungsleitungen.

ARP

Address **R**esolution **P**rotocol

Das ARP-Protokoll dient zur Adressauflösung. Es erfüllt die Aufgabe, zu einer gegebenen Protokoll-Adresse die korrespondierende Netzwerk-Hardware-Adresse (MAC-Adresse) herauszufinden.

Auf Hosts, auf denen die Internet-Protokoll-Familie benutzt wird, ist oft auch eine ARP-Protokoll-Implementation anzutreffen. Durch IP wird ein virtuelles Netzwerk mit Hilfe der IP-Adressen gebildet. Diese müssen beim Transport der Daten auf die gegebenen Hardware-Adressen abgebildet werden. Um diese Abbildung vorzunehmen, wird oft das ARP-Protokoll benutzt.

Bandbreite

Maximaler Durchsatz einer Verbindungsleitung (Angabe normalerweise in bps).

Broadcast

Eine Broadcast-Übertragung entspricht einem Rundruf: Über ein Broadcast-Telegramm werden alle Teilnehmer erreicht, die für Broadcast-Telegramme empfangsbereit sind.

Broadcast-Adresse

Ein Rundruf bzw. Broadcast in einem Computernetzwerk ist eine Nachricht, bei der Datenpakete von einem Teilnehmer aus an alle Teilnehmer eines Netzes übertragen werden. Soll eine Nachricht an alle Teilnehmer in einem Netzwerk gesendet werden, so wird als Zieladresse eine Broadcast-Adresse verwendet.

DFS

Dynamische Frequenzwahl (**D**ynamic **F**requency **S**election). Mit Hilfe der Dynamic-Frequency-Selection-Funktion, die ebenfalls Bestandteil der 802.11h-Erweiterung ist, kann ein automatischer Kanalwechsel vollzogen werden, falls während eines Betriebes auf einem Kanal ein anderer Nutzer beziehungsweise eine technische Einrichtung entdeckt wird. Dazu zählen beispielsweise Radarsysteme, die ebenfalls im 5-GHz-Frequenzband Daten übertragen. Deshalb wird vor jeder Kanalnutzung geprüft, ob kein anderes System bereits den Kanal beziehungsweise Frequenzbereich nutzt. Wird ein anderer Nutzer entdeckt, so soll auf dem Kanal die Datenübertragung abgebrochen werden und ein Kanalwechsel zu einem freien Kanal erfolgen.
Dadurch soll eine Beeinflussung durch WLAN-Systeme, die laut 802.11a im 5-GHz-Band arbeiten, vermieden werden.

DHCP

Dynamic **H**ost **C**onfiguration **P**rotocol

Dienste

Angebotene Leistungen eines Kommunikationsprotokolls.

ESS

Extended **S**ervice **S**et. ESS ist eine Kopplung von zwei oder mehreren Funkzellen eines WLANs (BSS - Basic Service Set) zu einem größeren Mobilfunknetz.

Firewall

Ein oder mehrere Geräte, die den Datenzugriff auf miteinander verbundene Netzwerke entsprechend gegebener Sicherheitsbeschränkungen ermöglichen oder ausschließen.

Handover

Als Handover bezeichnet man einen Vorgang in einem Mobilfunknetz (zum Beispiel einem Mobilfunknetz nach IEEE 802.11), bei dem das mobile Endgerät (Client) während einer Datenverbindung von einer Funkzelle in eine andere wechselt oder von einem Kanal zu einem anderen.

HTTPS

Hyper**T**ext **T**ransfer **P**rotocol **S**ecure

Protokoll für die Verschlüsselung und Authentifizierung der Kommunikation zwischen Webserver und Webbrowser im World Wide Web.

HTTPS ist eine Erweiterung von HTTP für die geschützte Übertragung von vertraulichen Daten mit Hilfe von SSL.

IEEE

Institute of **E**lectrical and **E**lectronics **E**ngineers

IEEE 802.11

Standard für Mobilfunknetze im 2,4 GHz-Band mit Übertragungsraten bis 2 Mbit/s.

IEEE 802.11a

Standard für Mobilfunknetze im 5 GHz-Band mit Übertragungsraten bis 54 Mbit/s.

IEEE 802.11b

Standard für Mobilfunknetze im 2,4 GHz-Band mit Übertragungsraten bis 11 Mbit/s.

IEEE 802.11e

Erweiterung des Wireless LAN Standards zur Unterstützung von Quality of Service (QoS).

IEEE 802.11g

Standard für Mobilfunknetze im 2,4 GHz-Band mit Übertragungsraten bis 54 Mbit/s.

IEEE 802.11h

Der Standard IEEE 802.11a erweitert um TPC und DFS.

IEEE 802.11i

Der Standard beschreibt unter anderem die Methode WPA2, das Verfahren TKIP und den Verschlüsselungsalgorithmus AES. Mit IEEE 802.11i werden eine Reihe von Schwachstellen des Sicherheitsmechanismus WEP geschlossen.

IEEE 802.1x

Kern dieses Standards ist die Nutzung eines Radius-Servers als Authentifizierungs-Server. Außerdem wird bei IEEE 802.1x die gesamte Kommunikation verschlüsselt abgewickelt.

Industrial Ethernet

Ein Bussystem nach IEEE 802.3 (ISO 8802-2)

IP-Adresse

Die IP Adresse besteht aus 4 Bytes. Jedes Byte wird dezimal dargestellt und ist durch einen Punkt vom vorherigen getrennt. Es ergibt sich also folgender Aufbau, wobei für XXX eine Zahl zwischen 0 und 255 zu setzen ist (Dotted Decimal Notation): `XXX.XXX.XXX.XXX`

Die IP-Adresse besteht aus zwei Teilen, der Netzwerkadresse und der Endteilnehmeradresse. Dadurch ist es möglich, verschiedene Teilnetze zu bilden. Abhängig davon, welche Bytes der IP-Adresse als Netzwerkadresse und welche als Endteilnehmeradresse genutzt werden, kann eine IP-Adresse einer bestimmten Adressklasse zugeordnet werden:

Adressklasse	Kennzeichnung Adressklasse	Netzwerk-Adresse und Endteilnehmer-Adresse
A	Byte 1 (möglicher Wert 1 - 126) (Byte 1 ist das am weitesten links stehende Byte.)	Byte 2 bis Byte 4 Möglicher Wert jeweils 0 - 255. 0.0.0 darf nicht vergeben werden, 255.255.255 ist die Broadcastadresse.
B	Byte 1 (möglicher Wert 128 - 191) Byte 2 (möglicher Wert 0 - 255)	Byte 3 und Byte 4 Möglicher Wert jeweils 0 - 255. 0.0 darf nicht vergeben werden, 255.255 ist die Broadcastadresse.
C	Byte 1 (möglicher Wert 192 - 223) Byte 2 und Byte 3 (möglicher Wert jeweils 0 - 255)	Byte 4 Möglicher Wert 1 - 254. 0 darf nicht vergeben werden, 255 ist die Broadcastadresse.
D	Byte 1 (möglicher Wert 224 - 239) Multicast-Adressen	Byte 2 bis Byte 4 Möglicher Wert jeweils 0 - 255 0.0.0 darf nicht vergeben werden. Es gibt einige Multicast-Adressen mit einer Sonderbedeutung, z. B. 224.0.0.1 Alle Systeme des Subnetzes 224.0.0.2 Alle Router des Subnetzes

iPCF

Die **i**ndustrial **P**oint **C**oordination **F**unction ist ein Kommunikationsprotokoll, mit dem der Datenverkehr einer Funkzelle zwischen dem Access Point und den verbundenen Stationen gesteuert wird, um Kollisionen zu vermeiden. Mit iPCF kann der Datendurchsatz auch bei einer hohen Teilnehmerzahl optimiert werden. Zusätzlich ermöglicht iPCF einen sehr schnellen Wechsel der Funkzelle.

PST

Primary **S**etup **T**ool

QoS

Quality of Service (QoS) oder Dienstgüte ist eine allgemeine Bezeichnung, die das ordnungsgemäße Funktionieren aller zusammenwirkenden Komponenten eines Telekommunikationsnetzes bezeichnet. Je nach Kommunikationsstandard (zum Beispiel IP) werden Fehlerparameter erfasst und aufgezeichnet, mit denen der Betrieb der Technik laufend überwacht wird und die die Basis für eventuell nötige Wartungsmaßnahmen bilden. In allgemeiner Formulierung bezeichnet QoS die Gesamtheit der Qualitätsmerkmale eines Netzwerks aus der Sicht der Benutzer eines bestimmten Dienstes.

RADIUS

Remote **A**uthentification **D**ial **I**n **U**ser **S**ervice. Ein Verfahren, bei dem die Authentifizierung über einen separaten Server abgewickelt wird.

Roaming

Freie Bewegung von Wireless LAN Teilnehmern auch über die Grenzen der Funkzelle eines Access Points hinaus. Der Teilnehmer kann ohne merkliche Unterbrechung von einer Funkzelle in die nächste wechseln.

Server

Ein Server ist ein Gerät, oder allgemein ein Objekt, das bestimmte Dienste erbringen kann; aufgrund der Anforderung durch einen Client wird der Dienst erbracht.

SINEMA E

Für die Planung und Konfiguration von IWLAN-Anwendungen wird die Planungs-, Simulations- und Konfigurationssoftware SINEMA E eingesetzt. Mit ihrer Hilfe können IWLAN-Netze z.B. nach Abdeckung, Datenrate, Signal-Rausch-Verhältnis und Überlappung unter Berücksichtigung von Umgebungs- und Geräteeigenschaften visualisiert werden.

SNMP

Simple **N**etwork **M**anagement **P**rotocol. Standardisiertes Protokoll zum Austausch von Netzwerkmanagement-Informationen.

SSID

Als **S**ervice **S**et **Id**entifier (SSID) bezeichnet man die Kennung eines Mobilfunknetzes, das auf IEEE 802.11 basiert.

Subnetzmaske

Die Subnetzmaske legt fest, welche Anteile einer IP-Adresse der Netznummer zugeordnet werden. Der Netznummer zugeordnet sind die Bits in der IP-Adresse, deren korrespondierende Bits in der Subnetzmaske mit 1 belegt sind.

TCP/IP

TCP = Transport Connection Protocol; IP = Internet Protocol

TKIP

Temporal **K**ey Integrity **P**rotocol. Verfahren zum zyklischen Wechsel der Schlüssel bei WLAN.

TPC

Durch die Transmit-Power-Control-Funktion (TPC), die durch die 802.11h-Erweiterung für 5-GHz-Komponenten als ergänzende Funktion eingeführt wird, soll eine automatische Anpassung der Sendeleistung erfolgen. Hierbei werden Informationen der Dämpfungsverluste und des erwarteten Spielraums in der Empfangsleistung berücksichtigt. Ebenfalls soll über TPC sichergestellt werden, dass die maximal zulässige Sendeleistung eines Kanals, die durch die jeweils zulässigen Regulierungsbehörden festgelegt ist, von den Komponenten nicht überschritten wird. Über TPC wird nun versucht, dass zwischen den korrespondierenden Stationen oder zwischen einem Access Point und einer Station mit der minimal notwendigen Sendeleistung gearbeitet wird.

WBM

Web **B**ased **M**anagement. HTTP-basierte Konfigurationsmethode, bei der ein HTTP-Server im jeweiligen Gerät genutzt wird.

WDS

Wireless **D**istribution **S**ystem. Richtfunkstrecken zur Kopplung der Zugangspunkte für ein Extended Service Set (ESS).

WEP

Wired **E**qivalence **P**rivacy ist ein optionaler Bestandteil des IEEE 802.11-Standards. WEP legt Verfahren für die Authentifizierung und Verschlüsselung fest, die beide mit festen, im Gerät hinterlegten Schlüsseln arbeiten. Alle Geräte, die auf ein Netz zugreifen wollen, in dem WEP eingesetzt wird, müssen also vorher mit den gleichen Schlüsseln versorgt werden. Auch die Erneuerung der Schlüssel kann nur manuell erfolgen.

Wi-Fi

Wireless **Fi**delity. Spezifikation für drahtlose Netze.

Die Wi-Fi-Allianz ist ein Zusammenschluss von WLAN-Herstellern, die die Interoperabilität von WLAN-Produkten prüfen und zertifizieren. Wi-Fi ist eine Zertifizierung von WLANs nach 802.11b, die von der WECA, der WiFi-Dachorganisation, durchgeführt wird. Mit dieser Zertifizierung wird die Interoperabilität von WLAN-Produkten bestätigt, die dem Standard 802.11b gemäß arbeiten.

Die Wi-Fi-Allianz erarbeitet darüber hinaus Standards. So hat die WiFi-Allianz für noch nicht standardisierte Sicherheitsverfahren eigene Architekturen wie die WiFi Protected Architecture (WPA) entwickelt, um die Kompatibilität der verschiedenen Herstellerprodukte testen zu können.

Für Echtzeitübertragungen hat die Wi-Fi-Allianz Wi-Fi Multimedia (WMM) für Übertragungen mit garantierter Dienstgüte (QoS) spezifiziert.

WPA

Wi-Fi **P**rotected **A**ccess ist eine Methode, die durch die Wi-Fi Allianz spezifiziert worden ist, um die Sicherheitslücken von WEP zu schließen. Dabei ist die Authentifizierung durch einen Server (802.1x) fest vorgeschrieben. Durch den dynamischen Austausch der Schlüssel bei jedem Frame wird eine weitere Sicherheit eingebaut. Als Verschlüsselungsart kann zwischen TKIP (Temporal Key Integrity Protocol) und AES (Advanced Encryption Standard) gewählt werden.
Obwohl WPA niemals offizieller Bestandteil der Standardfamilie IEEE 802.11 wurde, hat es innerhalb kürzester Zeit eine sehr große Verbreitung gefunden. Dies gilt allerdings nur für das zuvor beschriebene Verfahren WPA unter Verwendung von TKIP. Die optional mögliche Implementierung von WPA auf der Basis von AES konnte sich dagegen nicht durchsetzen und besitzt daher keine Praxisrelevanz. Erst durch den Nachfolgestandard WPA2 hat AES eine praktische Bedeutung erlangen können.

WPA-PSK

WPA-PSK ist die abgeschwächte Version von WPA. Bei diesem Verfahren wird keine Authentifizierung durch einen Server durchgeführt, sondern anhand eines Passwortes. Dieses Passwort muss auf dem Client wie auf dem Server manuell konfiguriert werden. Nach Möglichkeit sollte auf das Verfahren WPA umgestellt werden, um eine höhere Sicherheit zu gewährleisten.

Index

A

ACL, 143
Ad-Hoc-Netzwerke, 14
Adopt MAC Address, 83
Antenna Gain, 130
Antennen, 131
ARP Table, 158
Authentifizierung, 98, 137

B

Bandbreitenreservierung, 66, 174
Basic Wizard, 76
Beacons, 129
Betriebsart und Ländereinstellung, 108
Blitzschutz, 47
Bridge Priority, 65

C

CLI-Befehle
  Symbolik Darstellung, 196
  Verkürzte Befehlseingabe, 196
CostCost, 163
C-PLUG, 26, 121

D

DHCP-Server, 109

E

E-Mail, 113
Empfängerempfindlichkeit, 278
Erdung, 48

F

FAULT, 213
Fault State, 117
Forward Delay, 161
Funkzugang, 15

H

Hello Time, 161
Hilfefunktion, 106
HTTPS, 76

I

IEEE 802.11, 20
IEEE 802.11a, 20
IEEE 802.11b, 20
IEEE 802.11g, 20, 134
IP, TCP/IP, ICMP, SNMP, 191
IP-Adresse, 78
iPCF Wizard, 76

L

Ländereinstellung, 198
Learning Table, 158
Leuchtdiodensimmulation, 107
Link Check, 175
Load & Save, 118

M

MAC-Filter, 172
Max Age, 161
Mehrkanal-Konfiguration, 16

N

NAPT, 166
NAT, 166
NEW, 106

O

Overlap AP, 187

P

Passwort
Zeichensatz, 89
PRESET-PLUG, 258
Priority, 162
Protocol Filter, 173

R

RADIUS, 102
Redundante Verbindung, 67
Refresh, 106
Reset Statistics, 107
RFC
RFC 1518, 70
RFC 1519, 70
Root-Bridge, 65
RTS/CTS, 129, 132

S

Security Wizard, 76
Sendeleistung, 129
Set Values, 106
Sicherheitseinstellungen, 93
Sicherheitskleinspannung, 48
SNTP, 117, 212
Spanning Tree, 159
Spanning Tree Ports Parameters, 161
Speichern
von Gerätedaten, 118
SSID, 94
Standalone-Konfiguration, 13
Storm Threshold, 166
Subnetz-Maske, 70

T

TTL, 109

V

Verschlüsselung, 139

W

WDS, 148
Web Based Management, 74
Wizards, 74
WPA, 140
WPA2, 101